



# THE EUROPEAN DATA PROTECTION REFORM IN THE LIGHT OF CLOUD COMPUTING

---

Master Thesis

Name: B.J.A. Schellekens  
Supervisors: Prof.mr. J.E.J. Prins and Dr. E. Kosta  
Place and date: Tilburg, January 2013

## ACKNOWLEDGEMENTS

I would like to express my gratitude to my supervisors Corien Prins and Eleni Kosta for their guidance, insightful input and critical comments.

A very special thanks goes out to my father and mother for their unlimited support.

<b>LIST OF ABBREVIATIONS</b> .....	5
<b>INTRODUCTION</b> .....	6
Research Question.....	7
Methodology.....	8
<b>1 DEFINITION OF CLOUD COMPUTING</b> .....	10
1.1 Definitions of Cloud Computing.....	10
1.2 Characteristics.....	11
1.3 Actors.....	12
1.4 Service Models.....	13
1.5 Deployment Models.....	15
1.6 Conclusion.....	15
<b>2 CURRENT SITUATION OF EU RULES REGARDING DATA PROTECTION</b> .....	17
2.1 Data Protection in Europe.....	17
2.1.1 Primary Law.....	17
2.1.2 Directives.....	18
2.2 Data Protection Directive.....	18
2.2.1 Scope.....	19
2.2.1.1 Personal data.....	19
2.2.1.2 Processing.....	21
2.2.1.3 Exemptions.....	21
2.2.2 Applicability.....	22
2.2.2.1 Definitions.....	23
2.2.2.1.1 Controller.....	23
2.2.2.1.2 Processor.....	25
2.2.2.2 Who is really in control?.....	26
2.2.3 National Law Applicable.....	27
2.2.3.1 Establishment in a Member State.....	27
2.2.3.2 National Law applies by Virtue of International Public Law.....	28
2.2.3.3 Use of Equipment on the Territory of a Member State.....	29
2.2.4 Transfer to Third Countries.....	31
2.2.5 Jurisdiction and Enforcement.....	32
2.3 Conclusion.....	34
<b>3 THE EUROPEAN DATA PROTECTION REFORM</b> .....	36

3.1	Background.....	36
3.2	The Choice for a Regulation.....	38
3.3	Scope.....	41
3.3.1	Material Scope.....	41
3.3.2	Territorial Scope.....	42
3.4	Controllers and Processors.....	44
3.5	Data Subjects and Personal Data.....	45
3.6	Consent.....	45
3.7	Right to be Forgotten.....	47
3.8	Right to Data Portability.....	50
3.9	Right to Object.....	52
3.10	Profiling.....	52
3.11	Data Protection by Design and by Default.....	53
3.12	Representatives.....	54
3.13	Documentation.....	54
3.14	Data Breach Notification.....	56
3.15	Data Protection Officer.....	56
3.16	Transfer to Third Countries.....	57
3.16.1	Transfers with an Adequacy Decision.....	57
3.16.2	Transfers by Way of Appropriate Safeguards.....	58
3.16.2.1	Binding Corporate Rules.....	58
3.16.3	Existing Decisions and Mechanisms.....	58
3.16.4	Derogations.....	59
3.16.5	Disclosures not authorized by Union Law.....	59
3.17	Supervisory Authorities.....	60
3.17.1	One-stop-shop.....	60
3.18	Conclusion.....	61
<b>CONCLUSION</b>	.....	<b>63</b>
Visualization.....	.....	69
<b>BIBLIOGRAPHY</b>	.....	<b>70</b>

# LIST OF ABBREVIATIONS

API	Application Programming Interfaces
BCR	Binding Corporate Rules
CRM	Customer Relationship Management
DPA	Data Protection Authority
DPD	Data Protection Directive
EC	European Commission
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
ENISA	European Network and Information Security Agency
EU	European Union
IaaS	Infrastructure as A Service
ICT	Information and Communications Technology
IDC	International Data Corporation
NIST	National Institute of Standards and Technology
OS	Operating System
SaaS	Software As A Service
SLA	Service Level Agreement
PaaS	Platform As A Service
WP	The Article 29 data protection Working Party

# INTRODUCTION

It is the ICT subject of the last few years: cloud computing. Nowadays, everyone is connected to the internet and working in 'the cloud'. Updating your profile on Facebook, using an online office application or uploading files to an online storage service, these are just small examples of the use of cloud services. Cloud computing is an import factor in modern businesses because it can cut costs drastically and gives small (start-up) companies the possibility to enter large markets without high, risky start-up costs. The significance of cloud computing will only grow in the future; the International Data Corporation (IDC) forecasts that 80% of new commercial enterprise apps will be deployed on cloud platforms<sup>1</sup> and one can state that cloud computing services are essential for the internet as we know it.

The European Commission acknowledges the importance of cloud computing and has the objective to 'unleash the potential of cloud computing in Europe' on its digital agenda. It has the ambition to have the European Union at the forefront of the development of cloud computing to have the benefits on the demand as well as on the supply side.<sup>2</sup> This is not without a proper reason; predictions are that a cloud-friendly approach will generate 250 billion Euros in GDP in 2020, which is 162 billion Euros more than the case without this approach. Extra cumulative impacts from 2015 to 2020 are estimated at 600 billion Euros. Moreover, an enormous growth in jobs is predicted: the number of cloud-related jobs could rise above 3.8 million, which is in huge contrast with the predicted 1.3 million in the case of non-intervention.<sup>3</sup>

One of the main barriers for the development and deployment of the cloud computing in Europe is said to be the current data protection legislation.<sup>4</sup> A key argument made in this respect is that the present data protection rules are outdated and thus hinder cloud computing. The Data Protection Directive was enacted in 1995, a year when the technological development of cloud computing was not yet foreseen. Data transfers were not as massive as they are now and less than one percent of European citizens was connected to the internet.<sup>5</sup> Despite the fact that the directive has *inter alia* the objective to promote the free flow of data, trade expansion, cross-border transfer of data and economic and social progress, an updated version of its principles and provisions is desirable to keep up with the rapid technological developments and consequently fulfill EU's ambitions "*to become a world cloud computing powerhouse*".<sup>6</sup>

To revise the data protection regime in light of new technological developments, the European Commission proposed a reform of the data protection legislation. It proposed, among others, a General Data Protection Regulation which should "*update and modernize*"<sup>7</sup> the current rules. According to the legislator, the proposed Regulation is technology neutral and ready for the

---

<sup>1</sup> Gens 2012.

<sup>2</sup> EC communication 2012 B.

<sup>3</sup> IDC 2012, p. 48 – 64.

<sup>4</sup> EC communication 2012 B, p. 8.

<sup>5</sup> As mentioned by Vice-president of the European Commission and EU Justice Commissioner Viviane Reding in her speech announcing the proposal of the data protection reform, available at <[http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en)>, last visited 30 January 2013.

<sup>6</sup> EC communication 2012 B, p. 16.

<sup>7</sup> Reding 2012, p. 119.

challenges of cloud computing. Furthermore, the new framework is announced as “A strong, clear and uniform legal framework at EU level will help to unleash the potential of the Digital Single Market and foster economic growth, innovation (...)”<sup>8</sup> and will besides its primary objective to protect the rights of individuals also “facilitate the free flow of data within the Union and the transfer to third countries and international organizations”.<sup>9</sup>

## RESEARCH QUESTION

This thesis will discuss if the aforementioned objectives are realized by the proposed Framework, thereby focusing on cloud computing. In analyzing and discussing the present as well as proposed framework, this thesis uses an approach that includes free flow of data, innovation, economic growth and the digital single market as essential factors in realizing and maximizing the benefits of using and sharing data by means of cloud computing. In other words, the emphasis is not so much on risks for data subject, but potential for technological innovation in the European Union. Can indeed the European data protection legislation ‘unleash’ the potential of cloud computing in Europe as set out as an objective on the Digital Agenda of the Commission? This will be done on the basis of the following research question:

---

*To what extent does the current data protection legislation affect cloud computing and will the changes made by the proposed data protection reform contribute to the EU’s ambition to become a world cloud computing powerhouse?*

---

To come to an answer to this question, the following sub questions will be researched:

- What is cloud computing?
  - o What characteristics of cloud computing are in particular relevant and problematic in light of the characteristics of data protection legislation?
- What are the current rules regarding data protection?
  - o How do these rules relate to cloud computing?
  - o What are the effects of these rules on the cloud computing business?
- What are the changes made by the proposed Data Protection reform?
  - o How will these changes affect cloud computing?
  - o What amendments to the proposed rules are deemed necessary given Europe’s ambitions regarding the development and deployment of cloud computing?

The answer to these sub-questions will be given in the first three chapters. The first chapter of this thesis will analyze the concept of cloud computing and give the characteristics, actors and categories of cloud computing and the relevance of these subjects with regard to data protection legislation.

---

<sup>8</sup> As mentioned by Vice-president of the European Commission and EU Justice Commissioner Viviane Reding in her speech announcing the proposal of the data protection reform, available at <[http://europa.eu/rapid/press-release\\_IP-12-46\\_en.htm?locale=en](http://europa.eu/rapid/press-release_IP-12-46_en.htm?locale=en)>, last visited 30 January 2013.

<sup>9</sup> Recital 5 of the proposed Regulation.

Subsequently, the current data protection framework, with the focus on the Data Protection Directive, will be discussed extensively to provide a good analysis of the rules which cloud computing actors have to comply with at the present day. The shortcomings and difficulties with regard to the challenges of cloud computing set out in the first chapter will be pinpointed.

The third and last chapter reviews the proposed reform package, with the main focus on the proposed Regulation because of its importance for the cloud computing sector. The chapter will discuss if the proposed legislation contributes to the EU's ambition regarding cloud computing and will also give recommendations to increase this contribution.

Finally, the last chapter will give a conclusion and the answer to the research question based on the analyses and discussions of the previous chapters. It will also summarize the recommendations from the third chapter.

## METHODOLOGY

To find the answer to the aforementioned research question and sub questions, a traditional literature research has been executed. A desk study analyzed primary sources (e.g. legislation, official policy documents and case law) as well as secondary sources. Blogs and other modern formats are used as well, but only when they are written by authors with high reputation in the academic world or cloud computing sector. For the reason of the legal, economical and technical nature of the subject of this thesis, the desk research used sources and (scientific) insights from different disciplines.

In the first chapter, mainly technical sources have been consulted. Leading definitions of cloud computing such as the ones proposed by the NIST and the expert group of the European Commission are reviewed and secondary sources regarding the concept of cloud computing written by academics are used. Also views from leading technical companies (e.g. Oracle and Hewlett Packard) are taken into account and cloud services which are popular at this moment are used as examples. The sources that are used in the first chapter are a few years old at most, to ensure that the analysis and discussion is up to date.

For the second and third chapter, the author primarily used the legislative texts of respectively the Data Protection Directive and the Proposed Regulation. The opinions of the Article 29 Working Party and European Data Protection Supervisor complemented with leading case law from the European Court of Justice are used to further analyze the legislation. Secondary sources such as books, articles and research papers are used to pinpoint the difficulties and challenges in this legislation with regard to cloud computing. For the same reason as above, recent literature is used when possible.

The purpose of chapter two and three is to discuss the legislation and pinpoint the challenges regarding cloud computing and the possible solution to these challenges. Therefore, the data protection frameworks are not discussed in full detail, analyzing their entire content. Instead, the chapters focus on the parts of the legislative texts that are significant for the cloud computing sector. Other legislation is only discussed briefly. A full analysis of the whole Data Protection Directive or proposed Regulation is not necessary either, hence, only the provisions which are



important in the light of cloud computing are discussed. This selection is made on the basis of the review of the legislative texts and the comments and criticism given in the used literature.

# 1 DEFINITION OF CLOUD COMPUTING

The technology behind cloud computing is far from new, however, many authors see the shift in computing infrastructure as a new and evolving<sup>10</sup> paradigm.<sup>11</sup> This makes it difficult to catch all the aspects of cloud computing in one standard definition. In the literature and industry, many authors have tried to give a definition of cloud computing<sup>12</sup>, each one slightly different than the other, but none have become a global standard. This is acknowledged by leaders of the cloud computing industry; for example, Andy Isherwood, HP's vice president for software services in Europe stated during a conference: *"A lot of people are jumping on the bandwagon of cloud, but I have not heard two people say the same thing about it, there are multiple definitions out there of 'the cloud'."*<sup>13</sup>

This chapter will not be another attempt to give a precise definition of cloud computing. However, it will sketch the scope of the definition of the cloud computing paradigm that is used in this thesis. First, a selection of definitions in the literature and the given characteristics will be discussed. Subsequently, the actors, service and deployment models will be listed. The chapter will be closed with a compact conclusion.

## 1.1 DEFINITIONS OF CLOUD COMPUTING

Many have tried to define cloud computing, some of their definitions are more used and important than others. An example of an often used definition is the (in the U.S.) official definition published by the National Institute of Standards and Technology (NIST) which is a non-regulatory federal agency within the U.S. Department of Commerce. The NIST definition is as follows:

*"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*<sup>14</sup>

There is no official definition of cloud computing in Europe. However, an expert group of the European Commission (hereafter: Expert group) published a report about the future of cloud computing, wherein a definition of cloud computing is given:

---

<sup>10</sup> Mell & Grance, 2011, p. 1.

<sup>11</sup> Vaquero et al. 2008, p. 50.

<sup>12</sup> Geelan 2009.

<sup>13</sup> Andy Isherwood, HP's vice president for software services in Europe at HP Software Universe show and conference in Vienna 2008, as cited in Colin Barker, 'HP dismisses cloud hype' (2008) available at <<http://www.zdnet.com/news/hp-dismisses-cloud-hype/255222>> last visited 30 January 2013. Another example is the quote from Oracle's CEO Larry Ellison: "The interesting thing about cloud computing is that we've redefined cloud computing to include everything that we already do. I can't think of anything that isn't cloud computing with all of these announcements." as cited in Dan Farber, 'Oracle's Ellison nails cloud computing' (2008), available at <[http://news.cnet.com/8301-13953\\_3-10052188-80.html](http://news.cnet.com/8301-13953_3-10052188-80.html)> last visited 30 January 2013.

<sup>14</sup> Mell & Grance, 2011, p. 2.

*“A ‘cloud’ is an elastic execution environment of resources involving multiple stakeholders and providing a metered service at multiple granularities for a specified level of quality (of service)”<sup>15</sup>.*

This definition is quite broad; there is also a more specific description given in the report:

*“(…), a cloud is a platform or infrastructure that enables execution of code (services, applications etc.), in a managed and elastic fashion, whereas ‘managed’ means that reliability according to pre-defined quality parameters is automatically ensured and ‘elastic’ implies that the resources are put to use according to actual current requirements observing overarching requirement definitions – implicitly elasticity includes both up- and downward scalability of resources and data, but also load-balancing of data throughput”<sup>16</sup>.*

Vaquero et al discuss the definition of cloud computing by analyzing more than twenty definitions published by several authors. After mentioning that the concept of the cloud is still changing, the following definition is proposed:

*“Clouds are a large pool of easily usable and accessible virtualized resources (such as hardware, development platforms and/or services). These resources can be dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization. This pool of resources is typically exploited by a pay-per-use model in which guarantees are offered by the Infrastructure Provider by means of customized SLAs.”<sup>17</sup>*

## 1.2 CHARACTERISTICS

Vaquero et al, the NIST and the Expert group included the characteristics of cloud computing in their publications. After analyzing these and other cloud computing facets published by other organizations and authors, gives the following list of characteristics which are applicable to the concept of cloud computing that will be used in this thesis.

To start with *virtualization*; the end user does not see the technical complexity of the cloud services when using them. The consumers only see the easy to use and location- and device independent front-end. The front-end has a complex back-end which is hidden by way of routing, aggregation and translation.<sup>18</sup> The services are often much more complex than simulated to the consumer. For example, when you are a user of Dropbox, it seems like you have your own hard disk where you can upload and download your files to and from. This is a virtual hard drive; in fact, your files are divided on different hard drives of several servers on different locations.<sup>19</sup> Cloud providers should, in the light of EU data protection laws, inform the consumers about this virtualization; it is important that the cloud provider is transparent to the end-users about what happens with the

---

<sup>15</sup> EC Expert Group Report 2010, p. 8.

<sup>16</sup> EC Expert Group Report 2010, p. 8 – 9.

<sup>17</sup> Vaquero et al. 2008, p. 51.

<sup>18</sup> EC Expert Group Report 2010, p. 15. Virtualization is not explicitly named as a characteristic in the NIST report, however, it is implied in the following words of the definition: *“(…) and released with minimal management effort or service provider interaction”*. Mell & Grance 2011 p. 2.

<sup>19</sup> <<https://www.dropbox.com/help/7/en>> last visited 30 January 2013.

data. This flows from the fact that transparency is one of the basic principles of EU data protection law.<sup>20</sup>

This last example is also applicable on the second characteristic: *resource pooling*, which the NIST describes as followed: “*The providers’ computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand*”<sup>21</sup>. Important to note is that resource pooling can create the independence of location<sup>22</sup>, which can be an important legal issue with regard to the competence of the EU and the applicability of the EU laws and more specific, data protection laws.

Another characteristic is *broad network access*. The cloud services have to be accessible through a network, which most of the times is the internet. The access to the services is possible via several platforms, such as laptops and smart phones at every place in the world where one has a connection to the internet, which stresses the global character of cloud computing.<sup>23</sup>

The fourth characteristic is *rapid scalability and elasticity*<sup>24</sup>. The services provided by cloud providers are scalable on demand. This means that when the consumer needs, for instance, more (up-scaling) or less (down-scaling) processor power or disk space, this will be provided. Because of the elastic nature of the services, the increase or decrease of the services is done within minutes after the request or even automatically (*on demand self service*<sup>25</sup>), which is vital for large scale systems.<sup>26</sup>

Due to this scalability and elasticity, most of the business strategies regarding cloud computing are based on the ‘*pay per use*’ model. The consumer does not pay a fixed price for the service anymore, but the price depends on what the consumer demands. When up- or down-scaling the services, the consumer also raises or lowers the price he has to pay. That way, the price is elastic as well.<sup>27</sup>

### 1.3 ACTORS

There are several actors and relations within the business of cloud computing. The provider, consumer and aggregator are the most important roles in the cloud computing business. There are several other stakeholders who have a role in the industry, but their role is not significant for this thesis.<sup>28</sup>

The *cloud provider* is the ‘owner of the cloud’ and thus offers the infrastructure or virtual machines and creates the infrastructure to deliver the services to customers through a network. When the term *software provider* is used, it refers to a cloud provider which offers Software as a Service. The

---

<sup>20</sup> WP 196.

<sup>21</sup> Mell & Grance, 2011, p. 2.

<sup>22</sup> Sometimes, the user can chose for location dependency, e.g. The country where the datacenters are located. Mell & Grance, 2011, p. 2.

<sup>23</sup> *Ibid*.

<sup>24</sup> Instead of ‘rapid’, one can also use ‘near instant’, e.g. in ENISA 2009, p.14.

<sup>25</sup> On demand self service is listed as an essential characteristic by the NIST; Mell & Grance, 2011, p. 2.

<sup>26</sup> EC Expert Group Report 2010, p. 13 and Mell & Grance, 2011, p. 2.

<sup>27</sup> Ambrust et al. 2009, p. 10-14.

<sup>28</sup> I.e. the cloud carrier, the cloud auditor and tool providers, integrators and consultants.

providers of IaaS and PaaS are often referred to as, respectively, infrastructure providers and platform providers.<sup>29</sup> The provider activities do not only exist of service deployment, orchestration and management, but also security, privacy and data protection are important.<sup>30</sup>

Another important actor in the cloud computing business is, of course, the *consumer*, who buys the services via diverse distribution channels. The consumer is the end user and the one who makes use of the direct results of cloud computing. Cloud users can be natural persons or companies and organizations.

In the cloud services market, the relation is not always as simple as a contract between the cloud consumer and cloud provider, often *cloud aggregators* (or *resellers*) are the link between them. They combine the services of providers and then sell it as a new package to the consumers. For this reason, the aggregators are sometimes referred to as ‘service broker’<sup>31</sup> or ‘cloud broker’<sup>32</sup>. The aggregator is a cloud consumer and cloud provider at the same time. It buys the services from cloud providers and, after the incorporation to a new product, he sells it to a consumer, and thus provides cloud services.

The role of the actors in the cloud computing business is of great significance; it is essential to know who is or who are using the data, especially in the light of accountability. For instance, under the current data protection directive, the distinction is made between the data controller, data processor and the data subject and each of them have other rights and duties. The plurality of controllers and processors, all with different aims, raises several issues, as Leenes puts it: *“The clear cut distinction between data controllers and their helpers, the processors, on one hand and the data subjects on the other, is no longer an adequate model of personal data processing. Nor is the idea that data is processed for a single, or limited set of purposes.”*<sup>33</sup> These issues will be discussed in more detail in the next chapter of this thesis.

## 1.4 SERVICE MODELS

Clouds can be divided in different kinds of service models; each service model describes the level of service provided by the cloud provider. Based on the Expert group report of the European Commission<sup>34</sup> and the NIST definition on cloud computing<sup>35</sup>, the following service levels can be considered as the main service models of cloud computing.<sup>36</sup>

To start with *Software as a Service (SaaS)*, where applications are running on a cloud infrastructure or platform which are accessible via a thin client interface (browser) or program interface. The consumer only has the possibility to manage some user-specific settings, because the provider does not accommodate cloud features; they only provide applications running ‘in the cloud’. SaaS is an alternative to having software running on local machines and good examples are online office

---

<sup>29</sup> The definition of SaaS, IaaS and PaaS will be given in the next paragraph.

<sup>30</sup> Liu et al. 2011, p. 7.

<sup>31</sup> Barros & Dumas 2006, p. 31 – 37.

<sup>32</sup> Liu et al. 2011, p. 3.

<sup>33</sup> Leenes 2010, p. 9.

<sup>34</sup> Leenes 2010, p. 9 – 10.

<sup>35</sup> Mell & Grance, 2011, p. 2-3.

<sup>36</sup> In the literature are small differences regarding the service levels, e.g. Robinson et al. 2011, p. 18.

applications (Google Docs), online CRM systems (SalesForce CRM), webmail (Google Mail) and Social Network Sites (Twitter, Facebook).

Second, *Platform as a Service (PaaS)* is the service level where a computable platform upon which the consumer can host and develop applications and services by using programming language and API's<sup>37</sup> is provided. The consumer can control the deployed applications and sometimes the application-hosting environment as well. However, the infrastructure (servers, OS, storage) is still in the control of the provider. Examples include Google App engine and Windows Azure.

The third model is the *Infrastructure as a Service (IaaS)*; Trough virtualization, providers accommodate scalable and manageable resources as service. These include storage, network, processing and other computing resources. The consumer can deploy and run software, such as applications and OS. Amazon S3 is an example of an infrastructure as a service.

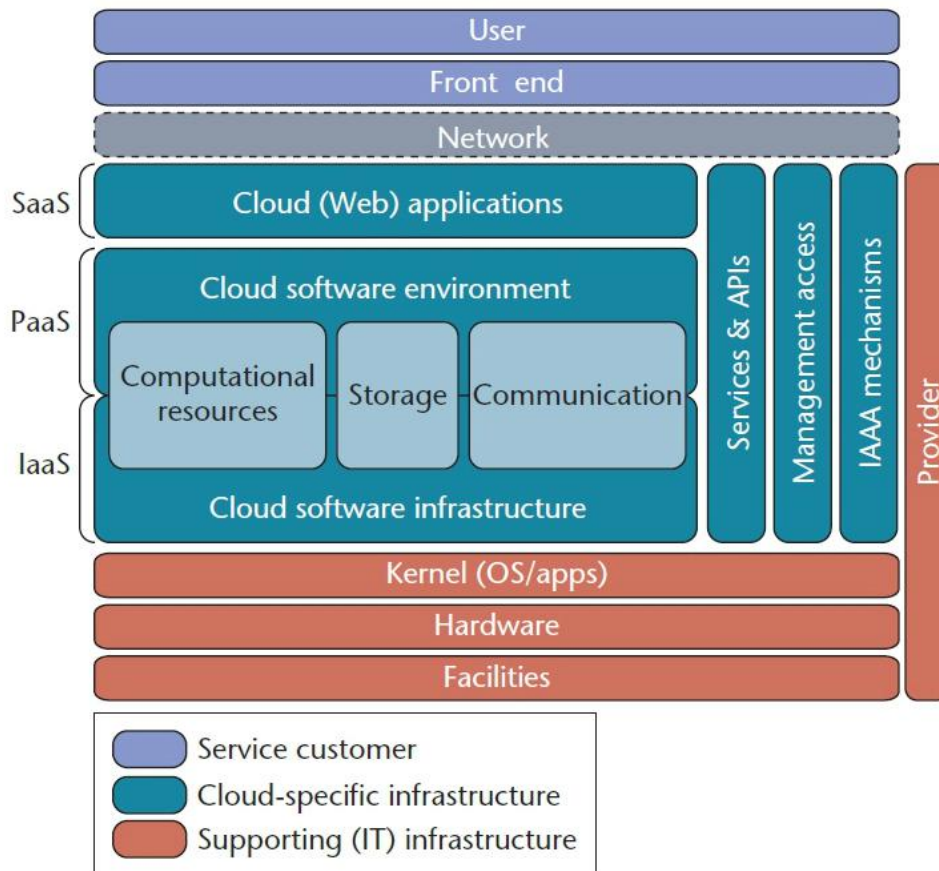


Fig 1. Cloud computing architecture<sup>38</sup>

<sup>37</sup> An application programming interface (API) “is a protocol intended to be used as an interface by software components to communicate with each other.”

<[http://en.wikipedia.org/wiki/Application\\_programming\\_interface](http://en.wikipedia.org/wiki/Application_programming_interface) > last visited 30 January 2013.

<sup>38</sup> Grobauer et al. 2011, p. 54. IAAA is the abbreviation for ‘Identification, Authentication, Authorisation and Accountability’, OS is the abbreviation for Operating System and for the definition of API’s, see nt. 29.

Sometimes, the application of the service models overlap and for this reason there is marginal difference in the definitions of the models in the literature. The European Commission gives an example of this in the expert group report regarding the future of cloud computing: “(...) *platforms typically have to provide access to resources indirectly, and thus are sometimes confused with infrastructures.*”<sup>39</sup>

## 1.5 DEPLOYMENT MODELS

One can also divide the cloud services in different deployment categories. Depending on the business model of the cloud provider, there will be a difference based on the exclusiveness of the service to the consumer.

The most exclusive deployment model is the *private cloud*. A private cloud service meets all the requirements of a cloud service and falls within the definition, but is only accessible by a number of parties within a private network. In the other corner of the deployment model spectrum is the *public cloud*. In this model, the cloud infrastructure is available for everyone: the general public.

There is also a deployment model which is less exclusive than a private cloud but more exclusive than a public cloud: the *community cloud*. The cloud is used by a group of organizations which have the same concerns (e.g. security, compliance) or mission. The cloud service is provided to a defined and limited number of parties.<sup>40</sup>

A combination of a public, community and private cloud is possible: the *hybrid cloud*. Despite the fact that there are not many hybrid clouds in use at the moment, the development is ongoing and base technologies are already introduced.<sup>41</sup> The hybrid cloud is a mix of the aforementioned clouds “*that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g. cloud bursting for load balancing between clouds)*”.<sup>42</sup>

Users of the public cloud have less control over the network than the private cloud users. Hence, the control over the rules regarding data protection is different; where the private cloud user can demand extra data protection provisions in the service level agreement, the users in the public cloud are usually not able to demand such a thing and just have to comply with the general terms and conditions of the cloud provider. This could lead to cases of vendor lock-in or problems with accountability, subjects which will be touched upon in the next chapters. The community and hybrid cloud have, obviously, more control than the public cloud but less than the private one.<sup>43</sup>

## 1.6 CONCLUSION

Despite the fact that many authors and companies in the business industry have tried to find one, there is still no standard definition of cloud computing. This chapter described cloud computing and its characteristics to understand the scope of the concept of ‘the cloud’ which will be used in this thesis.

---

<sup>39</sup> EC Expert Group Report 2010, p. 9.

<sup>40</sup> ENISA 2009, p. 15.

<sup>41</sup> EC Expert Group Report 2010, p. 11.

<sup>42</sup> Mell & Grance, 2011, p. 3.

<sup>43</sup> Leenes 2010, p. 2-3.

The essential characteristics of the cloud services are virtualization, resource pooling, scalability, elasticity, on-demand self service and broad network access. The main roles in the cloud business are the cloud provider, consumer and sometimes the aggregators. The business knows three service models and three deployment models.

The characteristics of cloud computing raise legal issues regarding the current data protection legislation; for instance, problems with the principle of transparency can be caused by virtualization, resource pooling leads to location-independence which has competence and legal enforcement consequences and the distribution of roles in the cloud business lead to difficulties with resolving the accountability question. The next chapters will analyze these problems in more depth and will discuss the provisions of the current and upcoming EU data protection legislation on these issues.



## 2 CURRENT SITUATION OF EU RULES REGARDING DATA PROTECTION

In the European Union, data protection rights are codified in primary and secondary law. This chapter will discuss the 1995 European framework regarding data protection and its effects on cloud computing. The main focus will be on the Data Protection Directive (DPD), given the general framework it poses and thus its importance relating to cloud computing business. But before embarking on this analysis, the broader scope of European legal sources and directives will very briefly be listed, to sketch the scope of data protection in Europe. Subsequently, the Data Protection Directive will be discussed and analyzed in light of the new challenges of cloud computing.

### 2.1 DATA PROTECTION IN EUROPE

#### 2.1.1 PRIMARY LAW

In Europe, the protection of privacy and data protection are fundamental rights, codified in the European Convention of Human Rights (ECHR)<sup>44</sup> and in the EU Charter of Fundamental Rights (EUCFR)<sup>45</sup>. The European Union acceded to the ECHR and the EUCFR has full legal effect since the Lisbon Treaty entry into force in 2009<sup>46</sup>. Privacy and data protection are not interchangeable concepts, although they partly overlap; this thesis discusses data protection legislation and its consequences on cloud computing and therefore, for practical reasons, it will from now on only focus on data protection and thus not discuss the privacy dimensions as well as the relation between both concepts.<sup>47</sup>

Article 6 of the Treaty on the European Union (TEU), which gives the EUCFR full legal effect in the Member states, is not the only primary law provision regarding data protection. Article 16 of the Treaty on the Functioning of the European Union (TFEU) confirms Article 8 EUCFR and states in sub two that the European Parliament and Council should create the legislation regarding the protection of the personal data of individuals, which resulted in, among others, the Data Protection Directive.

---

<sup>44</sup> Art 8: Right to respect for private and family life, European Convention for the Protection of Human Rights and Fundamental Freedoms.

<sup>45</sup> Art 7 Respect for private and family life and Art 8 Protection of personal data, Charter of Fundamental Rights of the European Union.

<sup>46</sup> Article 1(8) of the Lisbon Treaty states:

*“Article 6 shall be replaced by the following (...)*

*1. The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights of the European Union of 7 December 2000, as adapted at Strasbourg, on 12 December 2007, which shall have the same legal value as the Treaties.*

*(...)*

*2. The Union shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms. Such accession shall not affect the Union's competences as defined in the Treaties.(...)”.*

<sup>47</sup> For more information about the (inter)relation between privacy and data protection, see Bygrave 2001 and de Hert P. & Gutwirth 2009.

### 2.1.2 DIRECTIVES

The Data Protection Directive is the general framework regarding data protection, but it is not the only one. The Directive on privacy and electronic communications (E-Privacy Directive)<sup>48</sup>, which regulates the protection of personal data in the electronic communication sector, complements and particularizes the DPD.<sup>49</sup> The E-Privacy directive only applies to the activities of cloud providers, when they are processing personal data “in connection with the provision of publicly available electronic communications services in public communications networks in the Community”<sup>50</sup>. The directive contains provisions regarding, among others, traffic data, cookies and unsolicited communications (also known as ‘spam’). The Data Retention Directive<sup>52</sup> is worthy to mention as well, because it regulates the retention of data by telecommunication providers.<sup>53</sup> The applicability of the E-Privacy and Data Retention directives on (parts of) cloud computing services is debatable, for practical reasons this debate will not be discussed in this thesis, but one should keep in mind that there is a possibility that some activities of cloud providers falls under their regime.<sup>54</sup>

## 2.2 DATA PROTECTION DIRECTIVE

The most important piece of European legislation regarding data protection at the moment is the ‘Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data’ or in short, the Data Protection Directive. The aim of the directive is to ensure that personal data can move freely between Member States, but fundamental rights – such as the right to data protection – are safeguarded as well. In other words, it tries to balance the privacy of the individual on the one hand and the interests of the European internal market and thus the interests of commercial parties such as cloud computing businesses on the other. Also, it aims to guarantee the freedom of speech.<sup>55</sup> The Commission acknowledges the equal importance of the free internal market and the protection of fundamental rights, but states that, in legal terms, the internal market prevails.<sup>56</sup>

The Directive contains 33 articles and is based on a set of principles which have to be taken into account during the processing of personal data. These principles guarantee among others the purpose specification and limitation<sup>57</sup>, transparency<sup>58</sup> and proportionality<sup>59</sup>. The next paragraphs

---

<sup>48</sup> 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*), Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

<sup>49</sup> The full aim of the E-Privacy Directive can be found in its first article.

<sup>50</sup> Art 3 (1) E-Privacy Directive.

<sup>51</sup> WP 196, p. 6 – 7.

<sup>52</sup> Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105 , 13/04/2006 P. 0054 – 0063.

<sup>53</sup> De Hert & Papakonstantinou, 2011, 29-74 and WP 196, p. 6 – 7.

<sup>54</sup> Cloud Computing Hearing with Telecommunication and Web Hosting Industry 2011, p. 2 – 3, WP 196, p. 6 – 7.

<sup>55</sup> Article 1 DPD: *Objective of the directive* and Recital 3 of DPD.

<sup>56</sup> EC report 2003, p. 3-4.

<sup>57</sup> E.g. Art 6 (b) DPD.

will discuss the articles of the Data Protection Directive by subject that are of key importance in light of cloud computing; thus it will discuss the scope, the applicability, transfers to third countries and the enforcement of the directive and apply these subjects to the cloud computing business.

### 2.2.1 SCOPE

The scope of the directive can be found in the first chapter, in article 3 DPD to be exact. This article states that the directive *“shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system”*.<sup>60</sup> To analyze if the services of cloud providers fall into the scope of the directive, it is important to understand the wordings of article 3 DPD. A few things have to be made clear; what does this article mean in using the terms ‘personal data’ and ‘processing’?<sup>61</sup>

#### 2.2.1.1 Personal data

The second article of the Data Protection Directive gives the answer to the question of what ‘personal data’ means; sub a of article 2 gives the definition: *“any information relating to an identified or identifiable natural person”*. Where the identified or identifiable natural person is someone who can be (in)directly identified by a an identification number, for instance a national identification number<sup>62</sup>, or *“to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”*<sup>63</sup>.

The use of the words ‘any information’ is the result of the fact that the legislator wanted a broad notion of personal data, which follows, among others, from the Parliament’s wish to have the definition of personal data *“as general as possible”*<sup>64</sup>. The wide interpretation is confirmed in the opinion of the Article 29 Working Party (WP) regarding personal data. In this opinion, the WP discusses, inter alia, the nature, format and content of ‘any information’. The nature can be objective and subjective; it does not even matter if the information is the truth, and/or proven. Also the format is not restricted; every form that includes personal data is included in the personal data concept, which is a not an illogical opinion with regard to automatic processing. According to the Working Party, the content of ‘any information’ includes not only the sensitive data or data regarding the private and family life of the individual, *“but information regarding whatever types of activity are undertaken by the individual”*<sup>65</sup> as well. The broad notion is substantial in the case of

---

<sup>58</sup> For instance, the data subject should be informed of the purposes of the processing for which the data are intended, art 10 and 11 DPD.

<sup>59</sup> E.g. Art 6 (c) DPD.

<sup>60</sup> Article 3 DPD sub 1.

<sup>61</sup> The definition of a ‘filing system’ will not be discussed in this thesis, but the definition can be found in Article 2 sub c DPD and Recital 27 DPD.

<sup>62</sup> National identification numbers fall under a special category of processing, rules about this category can be found in section III of the DPD, and more specific regarding the national identification number: article 8 sub 7.

<sup>63</sup> Article 2 sub a DPD.

<sup>64</sup> COM (92) 422 final, 28.10.1992 (commentary on Article 2), p. 10.

<sup>65</sup> WP 136, p. 6.

cloud computing, because it leads to a high change of applicability of the directive on the services of cloud providers.<sup>66</sup>

Article 2 (a) DPD stipulates that the information must 'relate' to a certain person. The 'relating' part should also be explained broadly, according to the Article 29 Working Party. In the opinion about RFID chips, the working party stated: "*data relates to an individual if it refers to the identity, characteristics or behaviour of an individual or if such information is used to determine or influence the way in which that person is treated or evaluated*"<sup>67,68</sup>

This leads to the question: what falls under the definition of 'identified or identifiable'? As noted earlier, the process of identifying can be direct (by name) or indirect (by unique combinations). A person is identifiable when he can be distinguished from the others of the group to which he belongs on the basis of the processed personal data. This has to be analyzed on a case by case basis, for instance, an IP Address can fall in this definition (e.g. in a ISP log), but sometimes, it does not identify a person at all (when it is an address from a internet café PC). This possible unclearness leads to uncertainty.

Important to note is that "*to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*"<sup>69</sup>. In other words, the mere fact that it is possible to single out a person from a group does not mean he is 'identifiable' yet. The controller or another party must have, taken all the likely and reasonable factors into account, the intention to use the data. Examples of such factors are costs of the identifying process or the risks of technical failures and breach of the systems by a hacker. Another example is the storage time. This is a factor of relevance because a high end encryption in these days can for example be easy to crack in ten years time.<sup>70</sup>

Encryption is an important concept itself; when personal data is anonymized, it will no longer be identifiable. The directive is not completely clear about this<sup>71</sup>, but it is sure that an actor that is anonymizing personal data will fall within the scope of the directive. For instance, when a SaaS provider is making use of servers from a IaaS provider for a social network and the personal data on that social network is encrypted by the SaaS provider before it is put on the servers of the IaaS provider, then the activities of the SaaS provider will be in the directive's scope, but the activities of the IaaS will probably not.<sup>72</sup>

The final element of the definition of personal data is a 'natural person'. The definition of a natural person can be found in the various civil codes of the member states of the EU, but it is safe to say that a natural person is a living individual. Thus, dead persons are excluded from the protection of

---

<sup>66</sup> WP 136, p. 4, 6 – 9.

<sup>67</sup> Working Party document No WP 105: "Working document on data protection issues related to RFID technology", adopted on 19.1.2005, p. 8.

<sup>68</sup> For more info regarding the 'relating' part of the definition, see WP 136, p. 9 – 12.

<sup>69</sup> Recital 26 DPD.

<sup>70</sup> WP 136, p. 12 – 21.

<sup>71</sup> Recital 26 DPD: (...) *whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable (...)*.

<sup>72</sup> Hon et al. 2011 A, p. 221 – 228.

the data protection directive; the same applies to unborn children and legal persons. However, the member states have the freedom to extend the scope of the directive as long as no other Community law provision precludes it, as the European Court of Justice confirmed in the Lindqvist case.<sup>73</sup> For instance, Italy and Luxemburg have provisions protecting legal persons.<sup>74</sup> Moreover, personal data about a deceased or unborn individual or a legal person can still 'relate' to a living individual, as discussed above.

The fact that legal persons in principle do not fall under the scope of the DPD is relevant for the protection of, among others, industrial and trade secrets, financial information, know-how. These are important assets for companies and organizations that use cloud services. Nevertheless they fall outside the scope of the European protection regime. Lack of security could lead to the situation of compromised information and moreover, the cloud provider could link the information of several legal persons together to do a risk analysis and sell this to third parties. To prevent such complications and consequently a better protection for European entities, some authors have argued that the scope of European data protection legislation should be expanded to legal persons.<sup>75</sup>

### **2.2.1.2 Processing**

The definition of processing is given in sub b of article 2: *"'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction"*.

### **2.2.1.3 Exemptions**

Three exemptions from the scope of the directive are listed in sub 2 of article 3. Firstly, the processing of personal data during activities which do not fall within the scope of community law (such as title V and VI of the TEU). Secondly, the activities which fall under the following categories: public security, defense, state security and criminal law.<sup>76</sup> It should be noted that the distinction between these activities and normal commercial activities is not as clear as fifteen years ago; personal data is transferred from public entities to commercial cloud computing companies and back and forth.<sup>77</sup> The final exemption is in the case of processing of personal data by a natural person in a purely personal or household activity.<sup>78</sup>

As the current European Data Protection Supervisor Peter Hustinx stated in his speech regarding cloud computing: the household exemption could lead to uncertainty if a person's data is protected

---

<sup>73</sup> CJEU case C-101/2001, Bodil Lindqvist, 6 November 2003. (Lindqvist), para 98.

<sup>74</sup> For more info regarding the protection of personal data of legal persons, see Korff 2008.

<sup>75</sup> Pouillet et al. 2010, p. 13 – 14.

<sup>76</sup> Those fields fall in the scope of the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters and other legislation regarding (cyber)crime, for more info, see Bueno 2010, p. 117 – 123.

<sup>77</sup> EC Impact Assessment 2012, annex III; EDPS opinion 2012, p. 7. De Hert & Papakonstantinou, 2012, p. 132.

<sup>78</sup> Article 3 DPD sub 2.

when he uses the cloud only for pure personal activities.<sup>79</sup> The ECJ stated in the Lindqvist case<sup>80</sup> that the household exemption must be “*interpreted as relating only to activities which are carried out in the course of private or family life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people*” but did not touch upon the publication of personal data which is only accessible to a definite number of people, for instance in a private cloud deployment model. The way of functioning of cloud computing services creates a blur between the private and public use of data and therefore the question if the household exemption applies creates legal uncertainty in certain cases, especially because the consequences of applicability are extensive.<sup>81</sup>

One can conclude that cloud services fall within this definition of processing if it handles personal data (and no exemption is applicable); as was discussed in the previous chapter, the cloud computing business *is* about the environment wherein data will be processed. Therefore, regarding the scope of the directive in the case of cloud computing it is not the question if ‘processing’ takes place, but whether or not the data that is processed can be considered as personal data. As discussed above, the notion of personal data is quite broad in the perspective of the data protection directive. Mainly because of the broad definitions of ‘any information’ and how it can be ‘related’ and ‘identifiable’. It should be noted that the scope can be even broader in the member states, while each state has the freedom of implementation and is allowed to extend the scope. With regard to cloud services, one can conclude that significant amounts of personal data that travels around in the servers of cloud providers will probably fall under the scope of the directive. All the examples listed in the previous chapter (Gmail, Dropbox, Amazon Azure etc) could and most probably will contain personal data that has to be processed under the regime set out by the directive. Hence, one can conclude that the scope of the directive is reaching to the extent that it will apply to cloud services.

### 2.2.2 APPLICABILITY

The applicability of the directive is a subject heavily debated by scholars and legislators.<sup>82</sup> When does the directive apply and who is accountable? These are the questions to be answered in this paragraph and in answering them, specific remarks will be given as regards the status of cloud computing. The answer to the question when the national law (which is the implemented version of the directive) is applicable is given by article 4 DPD:

---

<sup>79</sup> "Data Protection and Cloud Computing under EU law", speech delivered by Peter Hustinx at the Third European Cyber Security Awareness Day, Brussels, available at <[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13\\_Speech\\_Cloud\\_Computing\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf)> last visited 30 January 2013.

<sup>80</sup> CJEU case C-101/2001, Bodil Lindqvist, 6 November 2003. (Lindqvist).

<sup>81</sup> Wong & Savirimuthu 2008.

<sup>82</sup> See for instance: Moerel 2011 A, Hon et al. 2011 C, Bygrave 2000, WP 56 and WP 179.

## Article 4

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;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

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

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

### 2.2.2.1 Definitions

To fully understand this article, one should be aware of the definition of 'controller' and its interaction with a 'processor'. Both are important concepts for the application of the directive on cloud services, because they determine the applicability of the directive, which national law is applicable and who is responsible when someone fails to comply with the data protection rules. The rights of the data subject are influenced by these concepts as well.<sup>83</sup> The definitions of the controller and processor will therefore be discussed now, with the focus on the most important concept of the two; the concept of the controller.<sup>84</sup>

#### 2.2.2.1.1 Controller

The concept of the controller is relatively old; it was shaped at the convention of the Council of Europe in 1981.<sup>85</sup> The concept of controller is codified in the data protection directive in sub d of article 2 DPD:

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or

---

<sup>83</sup> The rights of the data subject are codified in art. 10, 11, 12, and 14 DPD, all those articles create obligations for the controller or its representative.

<sup>84</sup> WP 169, p. 2 – 6.

<sup>85</sup> Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981 A few small changes were made to the definition after this convention. For instance 'controller of the file' is changed to 'controller'.

*regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;*<sup>86</sup>

In contrast to the data subject which can, in principle, only be a natural person, the legislator chose a broad interpretation of the personal side of the controller. Hence, the controller can be a “*natural or legal person, public authority, agency or any other body*”. The Article 29 Working Party states in her opinion that “*preference should be given to consider as controller the company or body as such rather than a specific person within the company or the body*”<sup>87</sup>. Even when there is a person in the company or public body solely responsible for the data processing activities, a common situation in the cloud computing business, he is still acting on behalf of the legal entity, and thus, the company or public body is the controller. The precise rules about when a natural person or the legal entity he is working for is responsible depend on national civil, criminal and administrative law.<sup>88</sup>

In the cloud computing business, there are often two or more companies who fit the definition of controller and this can lead to difficulties to determine who the responsible party is. Article 2 (d) DPD has a response on this situation, which can be found in the second part: “*alone or jointly with others*”. When drafting the directive, the legislator had not foreseen the complexity of the ICT nowadays, therefore, ‘jointly’ should not be interpreted as equal parties with equal responsibilities but as parties who work ‘together’ or are ‘not alone’, taking in account that the relationship between the parties will have different forms or combinations. It does not matter how many parties there are, as long as they can guarantee a full compliance of the data protection legislation, they have a certain freedom to divide and allocate the responsibilities and obligations which they got under the regime of the national data protection law. It has to be stressed that in the case of more than one controller, the situation can be so complex that it will conflict with the principle of fair processing due to the lack of transparency which is caused by the distribution of responsibilities, a situation which is not solved by the directive and a challenge for the new data protection framework.<sup>89</sup>

Having more information on who can be a controller, the subsequent question that arises is: *when* is one considered to be a controller? According to article 2 DPD it is the party “*which (...) determines the purposes and means of the processing of personal data*”. This description consists of two parts: ‘which determines’ and ‘the purposes and means of the processing of personal data’.

One should look to the factual circumstances of each case to decide which party is ‘determining’ the processing of personal data. As the Article 29 Working Party notes in its opinion, it is possible that indentifying the controller requires intensive research which will take a long time. However, WP 29 calls for such an interpretation of the directive that, in most situations, determines who the controller is in an easy and clear way, “*by reference to those - legal and/or factual - circumstances*

---

<sup>86</sup> Article 2 (d) DPD.

<sup>87</sup> WP 169, p. 15.

<sup>88</sup> WP 169, p. 15 – 17.

<sup>89</sup> WP 169, p. 17 – 23.



*from which factual influence normally can be inferred, unless other elements indicate the contrary*<sup>90,91</sup>

The next question which arises is what the controller has to ‘determine’; article 2 (d) DPD states ‘the purposes and means of the processing of personal data’ or in layman’s terms: ‘the why and how’ of processing activities. The essential question is the level of detail in determining the purposes and means and, subsequently, where the border has to be drawn between margin of maneuver of the processor and the determining of the controller. In its opinion, the art 29 Working Party stressed that the determining of the ‘purpose’ of the processing is the crux; the party that determines why the processing of personal data is taking place is, in principle, the controller. Determining the ‘means’ does not immediately mean that a party is a controller in the sense of article 2 (d) DPD. It depends on which ‘means’ are determined; WP 29 splits it in ‘means’ that can be well-delegated to the processor and means that have essential elements. Examples of well-delegable means are the technical ones, for instance, which software program should be used for CRM activities. The Working party provides illustrative questions such as ‘which data shall be processed?’ and ‘for how long shall they be processed?’ as examples for means with essential elements. Only when the means have essential elements which “*are essential to the core of lawfulness of processing*”<sup>92</sup>, a party can be identified as a controller.<sup>93</sup>

#### 2.2.2.1.2 Processor

The definition of ‘processor’ can be found in article 2 DPD as well. Sub e states:

*(e) ‘processor’ shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;*

The most important part<sup>94</sup> of sub e of article 2 DPD is the part stating ‘on behalf of the controller’, which means that, following from previous paragraphs, the purpose and essential means are determined by the controller. The processor does have a certain freedom in determining some technical and organizational means, as long as they are not essential to the core of the lawfulness of the processing, however as soon as a processor goes beyond this delegation, it will be identified as a controller. An example to illustrate this is the case of Gmail; the cloud application processes personal data as a processor for the activities as an e-mail provider, but becomes a controller when it uses the data of the e-mails for targeted advertising. Article 17 DPD requires that the relation between the processor and controller regarding data protection should be regulated by a legal act (*i.e.* a contract). This contract should – at least – stipulate that the processor should not go beyond its mandate given by the controller and that the processor is also obliged to comply with the security measures stated in sub 1 of article 17.

---

<sup>90</sup> WP 169, p. 9.

<sup>91</sup> More information regarding this interpretation, see WP 169, p. 7– 17.

<sup>92</sup> WP 169, p. 15.

<sup>93</sup> WP 169, p. 12 – 15.

<sup>94</sup> The part which describing the question who can be a processor will not be discussed here, because the explanation of “natural or legal person, public authority, agency or any other body” is the same as in the case of the controller, as discussed before. Furthermore, the definition of ‘processing’ and ‘personal data’ is given in an earlier paragraph about the scope of the data protection directive.

### 2.2.2.2 Who is really in control?

Applying the concepts of controller and processor in the cloud computing business is not easy, due to the complex structures, shared resources and the combined services of a range of providers by a cloud aggregator. Several parties could be controller and/or processor in different activities carried out for the purpose of a cloud service. A multitude of controllers and processors causes the risk that parties claim not to be responsible and do not comply or comply ineffectively with the data protection legislation and conflicts with the transparency principle.<sup>95</sup>

It can be even less transparent, when one argues that a cloud provider is neither a controller nor a processor for the main processing activities<sup>96</sup>, but just a provider of the technical facilities, i.e. a facilitator. Especially IaaS and PaaS providers are, essentially, merely providers of the (virtual) facilities and have no further idea what kind of data is on their machines and often they have no access to the data (e.g. when it is encrypted). Their services are just 'tools' for the controllers and processors of the data and should therefore not be considered as a processor, until they 'cross the line'.<sup>97</sup>

In practice, large public cloud service providers (e.g. Google, Apple, and Facebook) which act as a processor in a certain situation, have standard contracts and terms of service ready for the controller of the data. Those contracts are non-negotiable and therefore often called 'take-it-or-leave-it-contracts'. In that case, the end-user is the controller in theory, but he does not have that much actual power. The Working Party stresses that the end user is the one who decides to use a particular cloud service or not and thus, should choose a cloud provider which will comply with the data protection legislation applicable to the controller.<sup>98</sup> However, based on the popularity of the services of the above mentioned cloud companies, numerous consumers, companies are not avoiding those take-it-or-leave-it-contracts and are less in control than their classification of 'controller' would suggest.<sup>99</sup>

This lack of control by the end-user leads to several data protection risks, as set out in the discussed Opinion of the Working Party regarding cloud computing. First, it could lead to vendor lock-in when the end-user could have difficulties with the shifting of data from one cloud client to another, because each uses its own technology and standards. Secondly, the possibility of conflicting interests and objectives caused by the sharing of resources and virtualization could lead to a lack of integrity. Finally, due to the complex structure of some cloud networks, it can be hard or even impossible to intervene as a cloud client; for instance when the end-user did not receive the right tools and measures from the provider to access, edit or delete its data.<sup>100</sup> Solving the issues with the controller-processor model of the Data Protection Directive is one of the main challenges for the legislator to deal with while drafting new Data Protection legislation.

---

<sup>95</sup> Leenes 2010, p. 4 – 5 and WP 169, p. 7.

<sup>96</sup> As argued above, the cloud provider can be controller for non-primary processing activities, like the personal data which is processed during authentication and billing information.

<sup>97</sup> Hon et al. 2011 B, p. 11 – 23.

<sup>98</sup> WP 196, p. 8 – 9.

<sup>99</sup> Leenes 2010, p. 8 – 9; WP 169, p. 24 – 31.

<sup>100</sup> WP 196, p. 5 – 7.

### 2.2.3 NATIONAL LAW APPLICABLE

When the controller and processor are identified, the next step is to check if national law of a member state is applicable and if the answer is yes, which one. In the aforementioned article 4 DPD are three types of provisions regulating the applicability set out in sub a, b and c, these will be discussed in this paragraph.

#### 2.2.3.1 Establishment in a Member State

Sub 1 (a) of article 4 states that national law shall apply when the processing of personal data “*is carried out in the context of the activities of an establishment of the controller on the territory of the Member State*”. This provision is dividable in two parts; the first part regarding the processing carried out in the context of the activities and the establishment part. For practical reasons, the latter part will be discussed first.

On the basis of Article 50 TFEU and the jurisprudence of the European Court of Justice, the definition of an establishment involves “*both human and technical resources necessary for the provision of particular services are permanently available*”<sup>101</sup> and the “*the actual pursuit of an economic activity through a fixed establishment in another Member State for an indefinite period.*”<sup>102</sup>. Recital 19 of the directive adds that the establishment implies “*the effective and real exercise of activity through stable arrangements*”. This means that, for instance, a simple server in a member state does not constitute an establishment.<sup>103</sup> However, the form of an establishment is free, as long as it is a legal entity and fulfills the aforementioned requirements; therefore, a one-person office and a simple agent can also qualify as an establishment.<sup>104</sup>

If the controller has an establishment in the member state, the member state’s data protection law is applicable to its activities regarding data processing. This counts not only for the primary establishment (where the centre of activities of the controller are) but also for subsidiary establishments. The data protection directive, thus, does not apply the country of origin principle, despite the fact that this principle was applied in the proposal forms of the directive. Obviously, the risk of accumulation of applicable data protection laws is very high when a company is settled in more than one member state, which is confirmed in the second sentence of art. 4 (a) DPD: “*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*”. This is not a good example of a fully harmonized EU data protection, one of the purposes of the directive. For instance, a big company with cloud computing services like

---

<sup>101</sup> CJEU case 168/84, Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt, ECR [1985] p. 2251 (Bergholz), para14 and CJEU case C-390/96, Lease Plan Luxembourg SA v Belgian State, ECR [1998] p. I-2553.

<sup>102</sup> CJEU case C-221/89, The Queen v Secretary of State for Transport, ex parte Factortame Ltd and others, [1991] ECR I-3905. (Factortame).

<sup>103</sup> CJEU case C-390/96, Lease Plan Luxembourg SA v Belgian State, ECR [1998] p. I-2553. However, a server in a member state can lead to the applicability on basis of sub c of article 4 DPD.

<sup>104</sup> WP 179, p. 10 – 12.

Google has establishments in 16 member states of the European Union, each with its own – and possible slightly different – implementation of the directive.<sup>105</sup>

The first part of Article 4 (1) (a) DPD is even less transparent than the establishment part. The definition of processing was discussed before, but the question is when the processing is ‘carried out in the context of the activities of an establishment of the controller’.<sup>106</sup>

The article 29 Working party lists three considerations which should be taken in account. The degree of involvement of the establishment is the most important one; WP 29 proposes a ‘who is doing what’ test, where one should ask the question which activities are done by which establishment and if that activity triggers the applicability of national data protection law. It further notes that the nature of the activity will help to give an answer to the question which law will be applicable to which establishment. The overall objective is mentioned as a consideration as well; the effective protection of personal data in “a simple, workable and predictable way”<sup>107, 108</sup>

The Working Party admits that the situation of more than one applicable national data protection law is possible and responds with the notion that a functional approach is needed: “*it is their practical behaviour and interaction which should be the determining factors: what is the true role of each establishment, and which activity is taking place in the context of which establishment?*”<sup>109</sup> The Working Party does not discuss the fact that activities can overlap, which possibly results in an unworkable situation.<sup>110</sup>

### **2.2.3.2 National Law applies by Virtue of International Public Law**

Article 4 (1) (b) which states that national data protection law applies when the controller is not on the territory of the Member State but has to apply by virtue of international public law. This is, for instance the case at a foreign embassy, but also when a ship or airplane flies under a member state’s flag. One might say that it is not common at all that a ship or airplane is used to provide cloud services, but it is not as futuristic as it sounds. Google has filed a patent for a ship which has datacenters powered and cooled by seawater<sup>111</sup> and the most famous Torrent search engine Pirate Bay announced that is researching the possibility of having servers on GPS controlled drones.<sup>112</sup>

---

<sup>105</sup> Moerel 2011 A, p. 94- 97. For the current establishments of Google Europe see <<http://www.google.com/about/company/facts/locations/>> last visited 30 January 2013.

<sup>106</sup> There is a remarkable difference in the translations of article 4 of the directive, where the English version states ‘context’, the German, Dutch and French version use, respectively the terms ‘Rahmen’, ‘Kader’ and ‘Cadre’, which should be translated as ‘Framework’. Official translations of the data protection directive are available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT>> last visited 30 January 2013.

<sup>107</sup> WP 179, p. 14.

<sup>108</sup> WP 179, p. 12 – 13.

WP 179, p. 15.

<sup>110</sup> Hon et al. 2011 C, p. 11.

<sup>111</sup> <<http://www.zdnet.com/blog/btl/google-wins-floating-data-center-patent/17266>> last visited 30 January 2013.

<sup>112</sup> The Pirate Bay mentioned the use of drones in a blog post after small downtime, posted on 18-03-2012, available at <<http://thepiratebay.se/blog/210>> last visited 30 January 2013.

Placing servers on a ship or airplane can be useful to avoid the applicability of undesired tax law, strict intellectual property regulation or, of course, data protection legislation.<sup>113</sup>

### **2.2.3.3 Use of Equipment on the Territory of a Member State**

When the controller is not established on the territory of the Member State and national law does not apply by the virtue of international law, national law can still be applicable when the controller is making use of equipment for the purposes of data processing that is situated on the territory of the member state, as stated in article 4 (1) (c) DPD:

*“(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 State, unless such equipment is used only for purposes of transit through the territory of the Community.”*

This article is proof of the so-called long arm of the directive<sup>114</sup> and leads to complicated situations in the business of cloud computing, of which examples will be given hereafter, but first the article will be explained.

First, the controller should not have an establishment in a Member State. According to the opinion of the Article 29 Working Party, this part of the provision is relevant when there is no establishment for the purposes of article 4 (1) (a) DPD. Hence, art 4 (1) (c) applies when the controller has no establishment that is relevant for the activities in question in a Member State. The WP admits that this part of the article is not entirely clear and proposes its modification by the revision of EU data protection law, but for now it provides the opinion that sub c of art 4 (1) should apply *“where there is no establishment in the EU/EEA which would trigger the application of Article 4(1)a or where the processing is not carried out in the context of the activities of such an establishment”*.<sup>115</sup> This interpretation is needed to resolve the possible gap in the directive; art 4 (1) (a) speaks of a establishment which processing is carried out in the context of it activities and sub c of ‘not established on Community territory’, without the extensive interpretation of the Working Party, there would be a possibility that an establishment in a Member State would not be subject to the DPD.<sup>116</sup>

Secondly, the controller has to use automated or non-automated equipment for the purposes of the processing of personal data. The directive does not give a definition of equipment, the working party however states that the concept of equipment should be broad; it advises that the word ‘equipment’ should be interpreted as ‘means’.<sup>117</sup>

---

<sup>113</sup> Hon et al. 2011 C, p. 13. Also Embassies have to apply to their national data protection law, for instance, the Dutch Embassy in China, has to comply with the Dutch implementation of the DPD, WP 179, p. 17 – 18.

<sup>114</sup> Recital 20 DPD.

<sup>115</sup> WP 179, p. 19.

<sup>116</sup> For at good example, see Hon et al. 2011 C, paragraph 3.2.2.

<sup>117</sup> In translations of the directive, the translation of ‘means’ instead of ‘equipment’ is already used, for instance, in the French (‘Moyen’), German (‘Mittel’) and Dutch (‘Middel’) translations. Official translations of the data protection directive are available at <<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT>> last visited 30 January 2013.

The definition of ‘making use’ of equipment should be explained according to two elements: “*some kind of activity undertaken by the controller and the intention of the controller to process personal data*”<sup>118</sup>, thus, not every use of equipment directly leads to the applicability via art. 4 (1) (c) DPD.

Examples of equipment named by the working party are personal computers, tablets, terminals and servers. More controversial examples of equipment are cookies<sup>119</sup>, JavaScript<sup>120</sup>, banners and other similar applications, which extends the applicability of the directive a lot. An example of an American cloud mail provider with no establishment in a Member State can be used to explain the scope of this extension; when a Dutch person is using the mail service, it is responsible as the data controller of the personal data in the e-mails, as mentioned earlier. However, if the service provider is using the (personal) data in the e-mails the person receives and sends to put targeted advertising in their web application<sup>121</sup>, that company is responsible for that activity of processing of personal data on the basis of Art 4 (1) (c) DPD when it uses cookies or JavaScript applications with the purpose of storing and retrieving personal data of the Dutch person.<sup>122</sup>

An exemption on the ‘use of equipment’ concept can also be found in art 4 (1) (c); when the equipment is only used for “*purposes of transit through the territory of the Community*”, national data protection laws do not apply. One can think of telecommunication equipment used to transport data from state to state, such as cables and WIFI antennas. However, when personal data is processed during that transport, for instance a content filter in a private cloud network or the filtering of spam during the transmission, this exemption does not apply. The number of point to point transmission are decreasing, especially in cloud computing services and therefore, this exemption loses its functioning.<sup>123</sup>

According to sub 2 of article 4, when national law is applicable on the basis of article 4 (1) (c), the controller must designate a representative in the Member State which law is applicable. In practice, it is not clear whether a representative can be held responsible (with all the criminal and civil

---

<sup>118</sup> WP56, p. 9.

<sup>119</sup> The working party gives the following definitions of cookies: “*Cookies are pieces of data created by a web server that can be stored in text files that may be put on the Internet user’s hard disk, while a copy may be kept by the website. They are a standard part of HTTP traffic, and can as such be transported unobstructed with the IP-traffic. A cookie can contain a unique number (GUI, Global Unique Identifier) which allows better personalization than dynamic IP-addresses. It provides a way for the website to keep track of a user’s patterns and preferences. The cookies contain a range of URLs (addresses), for which they are valid. When the browser encounters those URLs again, it sends those specific cookies to the Web server. Cookies can also have a limited duration, the so-called session cookies*”. WP56, p. 10.

<sup>120</sup> A scripting programming language most commonly used to add interactive features to web pages, JavaScript runs on the Internet user’s computer rather than the web server’s computer. More info on <<http://en.wikipedia.org/wiki/JavaScript>> last visited 30 January 2013.

<sup>121</sup> This is not uncommon, for instance, one of the biggest free cloud mail providers, Google Mail (Gmail), is placing targeted advertising in its mail application: “In Gmail, ads are related to the content of your Google Account.” <<http://support.google.com/mail/bin/answer.py?hl=en&answer=6603>> last visited 30 January 2013.

<sup>122</sup> WP 179, p. 20 – 22 and WP56, p. 10 – 12.

<sup>123</sup> WP 179, p. 23.

consequences) or not. The working party acknowledges the practical problems with this provision.<sup>124</sup>

It is obvious that art 4 (1) (c) has a huge impact on cloud service providers which do not have an establishment in a Member State. Especially the SaaS providers will be subject to the directive easily, because they often use cookies, JavaScript applications and other scripts/programs which are used by the computers, tablets and smartphones of EU citizens. Cookies and JavaScript are so common on a website nowadays<sup>125</sup> that triggering the DPD on the basis of art 4 (1) (c) leads to large amount of non-EU cloud providers being subject to the data protection laws of all the 27 Member States, and on top of that, the cloud providers have to have a representative in each state on the basis of art 4 (2) DPD. It cannot be stressed enough that under the regime of the data protection directive, the application and scope should be determined on a case-to-case basis and with a practical approach, as mentioned before. For instance, an IaaS provider can be the responsible controller of the authentication service it has on its servers, but the end-user using the servers is the responsible party in the other data processing activities.

#### 2.2.4 TRANSFER TO THIRD COUNTRIES

In chapter four of the directive, the transfer to third countries<sup>126</sup> is regulated. Article 25 DPD states that a transfer to a third country should only be allowed when “*the third country in question ensures an adequate level of protection*”<sup>127</sup>. If the level of protection is ‘adequate’ should be “*assessed on a case by case basis in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations.*”<sup>128</sup>

The European Commission can issue an adequacy finding, where it states that a certain country fulfills the requirements of an adequate level of protection. Not many countries have acquired such an adequacy finding, because of the complicated nature of the procedure.<sup>129</sup> Other mechanisms can also be initiated by the Commission as well, such as the US Safe Harbor Framework.<sup>130</sup>

One can find more derogations in article 26 of the Data Protection Directive, for instance the exemption when the data subject gives his consent. However, this consent has to be given freely,

---

<sup>124</sup> WP 179, p. 23.

<sup>125</sup> Cookies are for instance used for authentication of the user, site settings, but also to track the user around the internet to see which site he is looking at and create a profile of that user which can be used for targeted advertising.

<sup>126</sup> Countries which have not implemented the directive.

<sup>127</sup> Art 25 (1) DPD.

<sup>128</sup> Art 25 (2) DPD, WP 12, p. 3, 5-7.

<sup>129</sup> Art 25 (6) DPD, Kuner 2012, p. 16, states which have obtained such a adequacy finding can be found at <[http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm)> last visited 30 January 2013.

<sup>130</sup> European Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce, [2000] OJ L215/7. For the US Safe Harbor Principles see [http://www.export.gov/safeharbor/eu/eg\\_main\\_018493.asp](http://www.export.gov/safeharbor/eu/eg_main_018493.asp) last visited 30 January 2013.

which will not be the case in, for instance, an employer – employee situation because of the relationship of authority, or a consumer ‘ticking the box’.<sup>131</sup>

Article 26 (2) gives the derogation by using contractual clauses which provide “*adequate safeguards with respect to the protection of personal data*”<sup>132</sup>. On the basis of art 26 (4), the commission can decide that certain standard contract clauses offer adequate safeguards. So far, the Commission has issued two sets of the so-called EU Standard Contractual Clauses.<sup>133</sup>

Finally, Binding Corporate Rules (BCR’s) are a solution for multinational groups of companies; these are internal rules (e.g. code of conduct) which are used to provide adequate safeguards for the protection of personal data when transferred to third countries. The main advantage of BCR’s is that not every time a company has to transfer data to another company of the same mother or corporation, it has to sign a standard contract.<sup>134</sup>

These ‘tools’ to transfer data to third countries seem unsuitable for the cloud computing business. The case by case procedure of art 25 DPD is obviously not working in a cloud service where much data is transferred each millisecond. The same goes for the EU Standard Contractual Clauses and mechanisms such as the safe harbor framework: these tools presume that data is transferred from point to point; this is rarely the case in the cloud. The adequacy finding of the European Commission is not a solution either, the data in cloud computing is often going from and to different countries, and on top of that, there are not that many states which have a qualified ‘adequate protection’.<sup>135</sup> Only the Binding Corporate Rules seem to be workable solution for multinational companies and organizations, but only when transferring data within the same companies/organization. One can conclude that the rules regarding transfers to third countries are limiting the free flow of data tremendously. Furthermore, the protection of personal data is not ensured if one takes the take-it-or-leave it contracts of large cloud computing companies into account.<sup>136</sup>

### 2.2.5 JURISDICTION AND ENFORCEMENT

On top of the aforementioned issues are other relevant issues following from the data protection directive. Jurisdiction is one of them: obviously, the DPD is not implemented in the national law of third countries; however, the directive can be applicable to cloud providers which are established in another country, the United States for example. The Working Party states that according to rules

---

<sup>131</sup> Moerel 2011 B, p. 154 – 155.

<sup>132</sup> Moerel 2011 B, p. 155

<sup>133</sup> <[http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm)> last visited 30 January 2013.

<sup>134</sup> The use of BCR’s are not codified in the DPD but acknowledged as a derogation under the regime of article 26 (2), see <[http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm)> last visited 30 January 2013. For more info regarding BCR’s, see Moerel 2011 B.

<sup>135</sup> The Commission has only recognized Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, State of Israel, Isle of Man, Jersey, the US Department of Commerce’s Safe harbor Privacy Principles, and the transfer of Air Passenger Name Record to the United States’ Bureau of Customs and Border Protection as providing adequate protection (so far). <[http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm)> last visited 30 January 2013.

<sup>136</sup> Balboni 2010, p. 8 – 9. And Pouillet et al. 2010, p. 22 – 25.



of international procedural law, a court in a Member State could claim jurisdiction because “*the party most concerned is the individual living on the same territory as the court*”<sup>137, 138</sup>

However, it is still questionable if the third country will recognize and enforce the verdict of the foreign judge. A controller with no establishment in Europe yet exposed to European data protection law on the basis of his website using cookies should not fear the European courts when breaching the data protection provisions, “*since there is no realistic chance of enforcement against it.*”<sup>139</sup> The coercive powers of the European Member States will only reach to local establishments or intermediaries when trying to control third country companies.<sup>140</sup>

This results in a large gap between the scope and applicability of the directive and the enforcement of it.<sup>141</sup> Kuner, in his article *Data Protection Law and International Jurisdiction on the Internet*, characterizes this gap as a *regulatory overreaching*: “*a situation in which rules are expressed so generally and non-discriminatingly that they apply prima facie to a large range of activities without having much of a realistic chance of being enforced*”<sup>142</sup>. He argues that data controllers and processors could see the European data protection legislation as a ‘bureaucratic nuisance’ instead of law. This development conflicts in his opinion with a solid protection of the personal data of European citizens.<sup>143</sup>

Another issue of relevance deals with access by non-EU enforcement agencies; personal data stored in datacenters in countries with less or even no protection of personal data with regard to law enforcement agencies could be accessed by these agencies, even without notification or procedure to object.<sup>144</sup> A ‘problematic example’<sup>145</sup> is the United States, where senior FBI agents have the ability to ask “*the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.*”<sup>146</sup> When an FBI agent has the court order to claim the European citizen’s personal data from a datacenter in the United States, the cloud provider has to provide this, without the consent or notification of the data subject or controller, which will constitute a breach of the right of the protection of personal data of the European citizen.<sup>147</sup>

---

<sup>137</sup> WP 179, p. 15.

<sup>138</sup> WP 179, p. 14 – 15.

<sup>139</sup> Kuner 2010, p. 235.

<sup>140</sup> Goldsmith & Wu 2008, p. 195.

<sup>141</sup> EC report 2003.

<sup>142</sup> Bygrave 2000, p. 255 as quoted in Kuner 2010, p. 236.

<sup>143</sup> Kuner 2010, p.228 – 236.

<sup>144</sup> Balboni 2010, p. 3.

<sup>145</sup> Pouillet et al. 2010, p. 22 – 23.

<sup>146</sup> 50 USC § 1861 - Access to certain business records for foreign intelligence and international terrorism investigations.

<sup>147</sup> Data is in principle not tangible, however, the servers or hard drives on which the data is stored can be claimed. American Civil Liberties Union. “*Reclaiming Patriotism: A call to reconsider the PATRIOT Act*”. ACLU, USA, 2009, p.32. Available at: <[http://www.aclu.org/pdfs/safefree/patriot\\_report\\_20090310.pdf](http://www.aclu.org/pdfs/safefree/patriot_report_20090310.pdf)> last visited 30 January 2013.

## 2.3 CONCLUSION

This chapter discussed the legal framework of the European Union regarding data protection and its relevance for cloud computing, with a main focus on the Data Protection Directive. The fact that data protection is a fundamental right in the EU and the extensive scope and applicability of the DPD show that the European legislator takes the right of data protection seriously.

However, the 17-year-old directive does not always adequately interact with new forms of technology deployment, such as cloud computing. The scope of the directive is far reaching, but excludes legal persons and is vague about encryption and anonymization. Moreover, the household exemption to the scope of the DPD is undesirable, given the legal uncertainty it can create.

Furthermore, it appears complicated to fit the cloud provider, aggregators and user in the concepts of controller and processor, which are decisive for the question if and which law applies and who is responsible for which part of the processing. The complex setting of the cloud environment and its actors results in a multitude of parties which can qualify as controller and/or processor for different activities, with the possibility that parties will claim not to be responsible. Sometimes, the cloud provider does not even fit within the scope of the directive, and is mere a facilitator. Another problem with the controller-processor model arises when the client of a service of a large cloud provider is the controller; it often does not have that much actual power, due to a take-or-leave-it contract provided by the processor.

The applicability of the directive can give even more problems, the case-by-case functional approach of researching which processing activity has to apply with which data protection law is complicated and can cost a lot of time. Moreover, due to the extensive scope of the directive, a SaaS provider which sets cookies on a computer of a European citizen has to comply with all the data protection laws of the Member States, each slightly different than the other. The definitions of an 'establishment' or 'context of activities' are still unclear, even after the opinions of the working party discussing these concepts.

Enforcement is not always possible when the company is not EU-based, depending on the willingness of the third country to recognize and enforce the judgment of a Member State's judge. This lack of enforcement could lead to foreign companies considering the European data protection legislation as a 'bureaucratic nuisance' instead of law. At the same time, enforcement agencies of third countries could have easy access to the data in the data centers of the cloud provider which is established in the specific third country. A problematic example of this is the USA patriot act.

Finally, the best examples that the legislator did not foresee the quick technology-related developments which resulted among others in applications such as cloud computing are the rules regarding the transfer to third countries. Article 25 DPD is obstructing the free flow of data and the 'tools' given by the articles in chapter IV of the DPD are not sufficient, except for the Binding Corporate Rules in the situation of a multinational company which transfers data between its subsidiaries.

One can conclude that the European legislator had many challenges during the drafting of the new data protection legislation, the next chapters will discuss whether the sketched problems regarding cloud computing are dealt with under the newly proposed European rules.

### 3 THE EUROPEAN DATA PROTECTION REFORM

On 25 January 2012, The European Commission (EC) proposed a comprehensive reform of the data protection framework. Vice-president of the European Commission and EU Justice Commissioner Viviane Reding speaks of an “updated and modernized” version of the principles enshrined in the current data protection directive.<sup>148</sup> According to the European Commission, the reform will be technology neutral, future-proof and ready for the challenges caused by the latest technological developments. The Commission explicitly mentions the cloud computing business as an example in its factsheet.<sup>149</sup> This chapter will pinpoint the updated or new rules which will affect the stakeholders in the cloud computing business and conclude if the shortcomings of the directive regarding cloud computing are covered. Furthermore, recommendations are given, which are deemed necessary given Europe’s ambitions regarding the development and deployment of cloud computing.

#### 3.1 BACKGROUND

Despite the fact that the Data Protection Directive was a milestone in data protection history, one has to admit that it has troubles regulating the free flow of data and the protection of personal data in the present time, as discussed in the previous chapter. The legislators cannot be blamed for this; at that time it was hard to foresee that the internet would grow as fast as it did the last fifteen years.

Knowing that a reform of the current data protection framework was needed, the commission needed more than two years of preparation and consulting to propose a new framework.<sup>150</sup> An impact assessment by the European Union concluded that there are three main problems with the current data protection framework: “*Barriers for business and public authorities due to fragmentation, legal uncertainty and inconsistent enforcement*”<sup>151</sup>, “*Difficulties for individuals to stay in control of their personal data*”<sup>152</sup> and “*Gaps and inconsistencies in the protection of personal data in the field of police and judicial cooperation in criminal matters*”<sup>153</sup>. These problems are discussed in detail in the previous chapter, except the problem on the protection of personal data in the field of

---

<sup>148</sup> Reding 2012, p. 119.

<sup>149</sup> EC Factsheet 2012, p. 1 – 2.

<sup>150</sup> Targeted consultations were organized in 2010 with Member State authorities and private stakeholders. In November 2010, EU Justice Commissioner Viviane Reding organized a roundtable on the Data Protection reform. Additional dedicated workshops and seminars on specific issues (e.g. data breach notifications) were also held throughout 2011; Public consultations, available at <[http://ec.europa.eu/justice/news/consulting\\_public/news\\_consulting\\_0003\\_en.htm](http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm)> last visited 30 January 2013 and <[http://ec.europa.eu/justice/news/consulting\\_public/news\\_consulting\\_0006\\_en.htm](http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm)> last visited 30 January 2013; EC Communication 2010; letter of EU Justice Commissioner Viviane Reding of 19 September 2011 to the members of the Article 29 Working Party, published at [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm) last visited 30 January 2013. As cited in EC communication 2012 A p. 3.

<sup>151</sup> EC Impact Assessment 2012, p. 11 – 20.

<sup>152</sup> EC Impact Assessment 2012, p. 21 – 31.

<sup>153</sup> EC Impact Assessment 2012, p. 31 – 37.

police and judicial cooperation in criminal matters, which, for the same practical reasons, will not be discussed in this chapter either.<sup>154</sup>

The commission proposed three possible solutions to solve these problems. The first solution was based on soft action, where only “very limited legislative amendments” would be made by the European legislator and encouraging standardization and self-regulation, interpretative communications, and technical support and funding by the EU would do the rest. The second option was a new modernized legal framework; new legislative proposals regarding the harmonization of substantive rules would be presented by the commission and certain provisions would be illuminated. The last option would be detailed rules at European level, which include a “*much more detailed EU legislation (...) and a centralized EU-level enforcement structure*”<sup>155</sup>. The Commission, which took the compliance costs and administrative burden into account, preferred the second option combined with some<sup>156</sup> soft action from the first and the abolition of notification which was proposed in the text of the third option.<sup>157</sup>

This option includes the fundamental reform of the whole data protection framework which is currently in use in the European Union. It is a process that will take at least five years, which is not exceptional. The law-making process of the Data Protection Directive took five years as well and replacing the framework cannot be done overnight due the high economical and human rights stakes.<sup>158</sup>

The proposal of the commission is a framework that consists of a Regulation setting out the general EU framework and replacing the Data Protection Directive and a Directive regulating the rules regarding judicial activities.<sup>159</sup> Due to the focus on cloud computing, the latter will not be discussed in this thesis. The proposed Regulation is of high importance for the cloud computing business and will be the main subject of this chapter. The full name of the proposed Regulation is: ‘the Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data’, or in short: ‘the General Data Protection Regulation’ (hereafter: the proposed Regulation).

The proposed framework should enhance “*individuals’ rights, the Single Market dimension of data protection and cutting red tape for business*”<sup>160</sup>, by ensuring a “*high level of data protection of individuals, the growth and competitiveness of EU industries, the operational effectiveness of the public sector (...) and a low level of administrative burden.*”<sup>161</sup>

---

<sup>154</sup> For more info regarding this subject, see EC Impact Assesment 2012, p. 31 – 37.

<sup>155</sup> EC Executive Summary of the Impact Assessment 2012, p. 7.

<sup>156</sup> “*The encouragement of privacy-enhancing technologies and certification schemes, and awareness-raising campaigns.*” EC Executive Summary of the Impact Assessment 2012, p. 9.

<sup>157</sup> EC Impact Assesment 2012, p. 63 – 78.

<sup>158</sup> De Hert & Papakonstaninou, 2012, p. 130.

<sup>159</sup> Furthermore, a “*limited number of technical adjustments*” will be made to the E-Privacy Directive and there will be some amendments to specific legislation to align them with the new framework, EC communication 2012 A, p. 4.

<sup>160</sup> EC communication 2012 A, p. 4.

<sup>161</sup> EC communication 2012 A, p. 12 – 13.

The intention of the European Commission is to finalize and adopt the new framework in 2014. This deadline is rescheduled, because the first one was highly optimistic.<sup>162</sup> The European Parliament, the Council and the European Commission will work closely together and other stakeholders (from the public and private sector) will be included in the dialogue regarding the reform.<sup>163</sup> The further lawmaking process is extensive and (major) changes to the proposal will not come as a surprise.<sup>164</sup> This chapter will discuss the proposal and the opinions of, among others, the Article 29 Working Party, the European Data Protection Supervisor, the Committee on Civil Liberties, Justice and Home Affairs, academics and cloud computing businesses, starting with one of the major changes, the choice for a regulation.

### 3.2 THE CHOICE FOR A REGULATION

As discussed in the previous chapter, one of the main problems of the current Data Protection Directive is the regulatory patchwork as a result of all the different national data protection laws and requirements in the European Union. The consequences of this fragmentation are worrying: unequal protection for European individuals, high costs and administrative burdens for controllers and processors and legal uncertainty for all the actors. International operating business, like cloud computing businesses, will have a disincentive to enter the European market and the patchwork of national data protection laws will affect the competitiveness of EU industries. It is therefore no surprise that the economic stakeholders stressed the need for harmonization during the consultations.<sup>165</sup>

For this reason, the new general legislation regarding data protection is a Regulation instead of a Directive. Regulations have direct effect (art 288 TFEU)<sup>166</sup> and consequently, there is no need for implementation by the Member States. As the most far reaching instrument of secondary EU law, the Member States are obliged to fully apply the Regulation and when national law conflicts with the provisions of a regulation, the regulation takes priority. *Ergo*: less fragmentation. The EC speaks of a “*harmonized set of rules*” which will “*reduce legal fragmentation and provide greater legal certainty*”.<sup>167</sup> However, despite the fact that the amount of pieces of the regulatory patchwork is reduced, the data protection legislation will still consist of several legislative pieces ‘sowed together’.

Firstly, Member States are allowed to adopt specific data protection provisions at domestic level that specify certain parts of the Regulation, but only in the circumstances given by the Regulation itself. For instance detailed sectoral laws: a national law regarding public health can lay down specific provisions with strict data protection rules. When several Member States have their own,

---

<sup>162</sup> EC communication 2012 A, p. 12; The first deadline to come to an agreement on the new framework in the end of 2012 is not achieved. Kuner 2012, p. 2.; The process will be an “*ordinary legislative procedure*” (article 16(2) TFEU) on the basis of article 294 TFEU, a procedure consisting of several complicated consultations between the Parliament and Council, see Craig & de Búrca, p. 123 – 129.

<sup>163</sup> EC communication 2012 A, p. 12.

<sup>164</sup> Kuner 2012, p. 2.

<sup>165</sup> See chapter 2; Explanatory memorandum of the Proposed Regulation, p. 2 – 4 and Reding 2012, p. 120 – 121.

<sup>166</sup> Craig & de Búrca, p. 105 – 106.

<sup>167</sup> Explanatory memorandum of the Proposed Regulation, p. 5 – 6.

each slightly different rules, a (limited and small) patchwork is created, which conflicts with the purpose of the choice for a Regulation and will have negative effects for the cloud computing business working in that specific area. It has to be noted though that the provisions made by the Member States have to be in line with the Regulation and will be adopted for the sake of coherence. Therefore, the variation of those provisions in domestic laws will be minimal.<sup>168</sup> However, the Member States have more room for their own data protection provisions. Specific laws regarding the processing in employment context and personal data concerning health may be adopted by the Member States<sup>169</sup>, States can limit the rights of the data subject<sup>170</sup> and profiling measures can be authorized by a Member State.<sup>171</sup> Even complementing the proposed Regulation is allowed in certain areas; recital 18 states that domestic rules regarding public access have “*to be taken into account when applying the provisions set out in [the] Regulation*”.<sup>172</sup> Furthermore, article 6 states that the processing of personal data is lawful when the processing is “*necessary for compliance with a legal obligation*”<sup>173</sup> or “*necessary for the performance of a task carried out in the public interest or in the exercise of official authority*”.<sup>174</sup> These are examples where the grounds of lawful processing can be purely based on national law, only limited by conditions regarding the quality of that law.<sup>175</sup> Consequently, Member States do not have the amount of leeway they had when transposing the Data Protection Directive because of the direct effect of a Regulation. However, they still have some room for maneuver in certain areas.<sup>176</sup> This will not be a problem as far as this room for maneuver is needed for the consistent application of the proposed Regulation, but improper use at some points is possible.<sup>177</sup>

Secondly, the Commission will be empowered to adopt delegated or implementing acts.<sup>178</sup> Despite the fact that such acts contribute to the harmonization and further align the national laws of the Member States, some issues arise. For instance, it is questionable if all the delegated acts in the proposed Regulation are restricted “*to supplement or amend certain non-essential elements of the legislative act*” as article 290 (1) TFEU demands. Examples are the provisions regarding the notification of a data breach. The criteria and requirements for establishing the data breach and for the particular circumstances in which a controller and a processor are required to notify the personal data breach will be further specified by the Commission. However, these are essential elements of the proposed Regulation and should therefore be specified in that act, not only for compliance with article 290 (1) TFEU, but for preventing legal uncertainty as well. This uncertainty will increase substantially when the acts are not all adopted when the proposed Regulation enters

---

<sup>168</sup> Reding 2012, p. 121. See also CJEU case 230/78 *SpA Eridania-Zuccherifici nazionali and SpA Società Italiana per l'industria degli Zuccheri v Minister of Agriculture and Forestry, Minister for Industry, Trade and Craft Trades, and SpA Zuccherifici* [1979] ECR02749, paras 33, 34 and 35.

<sup>169</sup> Art 81 and 82 of the proposed Regulation.

<sup>170</sup> Art 21 of the proposed Regulation.

<sup>171</sup> Art 20 (2) (b) of the proposed Regulation.

<sup>172</sup> Recital 18 of the proposed Regulation.

<sup>173</sup> Article 6 (c) of the proposed Regulation.

<sup>174</sup> Article 6 (e) of the proposed Regulation.

<sup>175</sup> Article 6 (3) of the proposed Regulation; EDPS opinion 2012, p. 9.

<sup>176</sup> Reding 2012, 120 – 122.

<sup>177</sup> EDPS opinion 2012, p. 7 – 9.

<sup>178</sup> This can be found in many provisions of the proposed Regulation. See chapter X of the proposed Regulation for the general provisions regarding this empowerment.

into force. The enforcement of the proposed Regulation will be difficult as well when not all the acts are in place. Taking into account that there are 45 envisaged acts, this does not seem unrealistic.<sup>179</sup> The legislator should review all the articles where it gave the Commission the power to adopt delegated and implementing acts and reconsider if the powers are really necessary or even legal in the light of article 290 (1) TFEU. Alternatives are the recitals or the proposed Regulation itself. Guidance by the European Data Protection Board (the former Article 29 Working Party) is an alternative as well.<sup>180</sup>

Furthermore, the proposed framework does not cover the processing of personal data in the electronic communications sector. The E-Privacy Directive continues to exist and to govern subjects such as traffic and location data by electronic communication services. The same goes for the Data Retention Directive, which is linked to the E-Privacy Directive and covers the retention of personal data. As stated in the previous chapter, cloud computing business could<sup>181</sup> fall into the scope of the E-Privacy Directive and Data Retention Directive and those businesses will still to encounter the negative effects of the division between a general data protection framework and the independent sector specific directives. The regime for service providers in the electronic communication business will be different in comparison with other service providers which fall under the scope of the proposed Regulation, for instance in the case of location data. Moreover, both directives are transposed in the national laws of the Member States causing more fragmentation. Of course, this is not a new problem, but one might have expected that the Commission would propose at least a way to let the directives be subsidiary to the Regulation, with or without making new rules<sup>182</sup>, to fulfill the goal of establishing a “*comprehensive personal data protection scheme covering all areas of EU competence*”<sup>183,184</sup>

Finally, the data protection legislation in Europe will still be fragmented in other fields after the proposal. The processing of personal data in the context of national security and common foreign and security policy falls outside the scope of EU law, and thus, it will not be covered by the regulation. The processing by EU institutions, bodies and agencies will remain subject to Regulation No 45/2001. The proposed framework still makes a distinction between general/commercial data protection and the protection of personal data that is security-related. This does not seem to be a wise choice, because the data processed by private cloud computing companies can be used for national security and even the other way around.<sup>185</sup> The European Data Protection Supervisor (EDPS) expressed his concerns regarding this issue in his opinion on the reform package. With

---

<sup>179</sup> EDPS opinion 2012, p. 12 – 13.

<sup>180</sup> LIBE draft report 2013, WP 199, p. 8 – 12. The Working Party also suggests the alternative of national law, but this will conflict with the harmonization and therefore lose its usefulness for the cloud computing actors. See also the Annex of WP 199 where the Working Party discusses the alternatives article by article.

<sup>181</sup> As mentioned in the previous chapter, there is a debate about the applicability of the E-Privacy and Data Retention directives on (parts of) cloud computing services. For practical reason, this debate will not be discussed in this thesis. Cloud Computing Hearing with Telecommunication and Web Hosting Industry 2011, p. 2 – 3, WP 196, p. 6 – 7.

<sup>182</sup> New rules would be desirable, e.g. making the e-privacy directive technology neutral, for more see Korff 2012, p. 11 – 17.

<sup>183</sup> EC communication 2012 A, p3.

<sup>184</sup> Korff 2012, p.3 – 17.

<sup>185</sup> Art 14 of the proposed Framework Decision. De Hert & Papakonstantinou, 2012, p. 132.



examples such as the transfer of Passenger Name Records (PNR)<sup>186</sup> and financial data transfers the EDPS proves that the borders between private and public sector are becoming more and more blurred. A development which the Commission touched upon in its Impact Assessment, but it did not use the opportunity to solve the legal uncertainty which is created by situations described in this paragraph.<sup>187</sup>

One can conclude that the European Commission's choice for a Regulation is the right one; the negative effects of the regulatory patchwork created by the DPD are reduced substantially. However, Member States still have some room of maneuver, given by the proposed Regulation. Also the empowerment of the commission to adopt delegated or implementing acts has negative consequences, especially when the acts are not adopted yet when the Regulation applies. Furthermore, the E-Privacy and Data Retention directives are not reformed at all, while making it subsidiary to the proposed Regulation would be desirable. Finally, maintaining the legislative distinction between commercial and security-related processing is a choice which does not stroke with the reality: personal data is flowing from cloud computing providers to national agencies and back and forth.

The Commission did not achieve full harmonization and this will have effects on cloud providers. At this point, it cannot be foreseen what the amount of secondary legislation is going to be, with the result that it is not possible yet to estimate the real consequences to cloud providers. Nevertheless, the Commission should put more effort in reaching the goal of full harmonization, which is necessary in these times of cross-border data transfers and the globalization of technology (e.g. cloud computing). It should review the provisions where the Member States or itself has the power to adopt implementing and delegated acts and check whether the consequences of this power will not maintain the issues regarding the 'regulatory patchwork' of the current framework. The Commission should prevent that the proposed Regulation would become a 'black box'.<sup>188</sup> Also recommended is amending the E-Privacy and Data Retention directive and making them at least subsidiary to the proposed Regulation. Amending Regulation (EC) No 45/2001 to at least such an extent that it will be consistent with the proposed Regulation is also desirable.

### 3.3 Scope

#### 3.3.1 MATERIAL SCOPE

There are no significant changes to the material scope, which is currently governed by article 3 DPD and will be replaced by article 2 of the proposed Regulation. One should, however, note sub d of article 2 (2), which governs the household exception<sup>189</sup>:

---

<sup>186</sup> For more information regarding PNR, see the webpage of the European Commission on this subject, available at <[http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/passenger-name-record/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/passenger-name-record/index_en.htm)> last visited 30 January 2013.

<sup>187</sup> EC Impact Assessment 2012, annex III; EDPS opinion 2012, p. 7, LIBE draft report 2013, p. 210 – 211.

<sup>188</sup> Peter Blume states that the Regulation in the form of the proposal already resembles a black box to some degree. See Blume 2012 p. 130 – 136; EDPS opinion p. 8 – 14.

<sup>189</sup> Currently found in article 3 DPD.

## Article 2 (2)

*This regulation does not apply to the processing of personal data:*

*(...)*

*(d) By a natural person without any gainful interest in the course of its own exclusively personal or household activity;*

*(...)*

By only adding the ‘gainful interest’<sup>190</sup> fragment, the European Commission fails to fill the gap which is made by the household exemption. The exemption creates, as explained in chapter two, the uncertainty of whether a person’s data is protected when using a cloud service pure for personal activities.<sup>191</sup> According to the Article 29 Working Party this leads to an undesirable situation: “*The result is a situation of lack of safeguards which may need to be addressed, particularly given the increase in the number of such situations.*”<sup>192</sup>

Recommended is to follow the thoughts of European Data Protection Supervisor Peter Hustinx, who vouched for an explicit requirement which bounds cloud businesses to the same requirements as regular data processors when providing a service to a natural person whose processing falls into the scope of the household exemption.<sup>193</sup> In that case, the service of the provider has to comply with the principles and security measures of the Regulation and the person’s data protection rights are protected. This is already done in recital 15 of the proposed Regulation, which – despite the obvious mistake of not deleting the word ‘also’- states that “*the exemption should also not apply to controllers or processors which provide the means for processing personal data for such personal or domestic activities.*” This sentence should be added to article 2 (2) (d) to stress the importance of it. Furthermore the word ‘also’ should be deleted, for the reason that it is an obvious mistake made by the legislator.<sup>194</sup>

### 3.3.2 TERRITORIAL SCOPE

Contrary to the material scope, there are some substantial changes made to the territorial scope of the data protection legislation. The basic rule of article 4 (a) DPD is maintained, sub 1 of article 3 of the proposed Regulation (territorial scope) formulates the concept like this: “*This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.*”<sup>195</sup> There is however, a turnover on the level of jurisdiction. The Data Protection Directive, as pointed out in chapter two, creates a lot of confusion in this field

---

<sup>190</sup> An unwanted addition: “*The processing of personal data by a natural person for private and household purposes can sometimes have a gainful interest (e.g. when selling private belongings to other private persons) but still should fall outside the scope of the Regulation as long as there is no connection to a professional or commercial activity.*” LIBE draft report 2013, p. 62.

<sup>191</sup> See chapter 2, para 2.2.1.3.

<sup>192</sup> WP 168, p. 18.

<sup>193</sup> “*Data Protection and Cloud Computing under EU law*”, speech delivered by Peter Hustinx at the Third European Cyber Security Awareness Day, Brussels, available at <[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13\\_Speech\\_Cloud\\_Computing\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf)> last visited 30 January 2013.

<sup>194</sup> Or the word ‘exemption’ should be replaced by ‘regulation’. See EDPS opinion 2012, p. 16.

<sup>195</sup> The applicability of European Data protection law by virtue of international law is not changed as well. See article 3 (3) of the proposed Regulation and chapter 2, para 2.2.3.2.

by claiming jurisdiction when a controller makes use of 'equipment' on the territory of a Member State.<sup>196</sup> The European Commission left this concept and created a new test for the jurisdiction over foreign data controllers. This test can be found in article 3 (2):

*This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:*

*(a) the offering of goods or services to such data subjects in the Union; or*

*(b) the monitoring of their behaviour.*

As can be read in the article, the confusing 'use of equipment' is abandoned and two categories of processing activities are listed. The first one is the offering of goods or services, which is the substitute of the former inter-version 'activities directed at the data subject' category. 'Directed activities' is a concept which is really hard to define, especially given the rapid technological development and therefore the concept of 'the offering of goods or services' is better choice. However, the concept of sub a still leaves some room for interpretation.<sup>197</sup>

For instance, the Commission should made clear that payment of the goods and services that are offered is required. Many cloud services are providing their services for free, creating revenue on the basis of (targeted) advertisements, it should be clear that these services fall under the scope of the proposed Regulation as well.<sup>198</sup>

The 'monitoring of behavior' category is clarified by recital 21 of the proposed Regulation:

*(21) In order to determine whether a processing activity can be considered to 'monitor the behaviour' of data subjects, it should be ascertained whether individuals are tracked on the internet with data processing techniques which consist of applying a 'profile' to an individual, particularly in order to take decisions concerning her or him or for analysing or predicting her or his personal preferences, behaviours and attitudes.*

It is clear that sub b is targeted at companies that are 'profiling' individuals on the internet, mostly done by digital marketers. Individuals are being tracked on the internet by companies as Google or social media networks like Facebook (and many others) with the purpose to sell the information to advertisers which can show targeted advertising on the websites the individual is visiting.<sup>199</sup>

There is one problem with this article on the territorial scope that has to be pinpointed as well, especially with regard to the trans-border aspect of cloud computing. Article 3 only regulates the scope of *the Regulation*, and does not mention national law. As can be read above, the proposed Regulation leaves some room for maneuver for the Member States, especially for sectoral laws. It is uncertain how far the national laws apply to the data processing activities of a controller from another (European) state. This legal uncertainty should be solved by the Commission because

---

<sup>196</sup> See chapter 2, para 2.2.3.3.

<sup>197</sup> WP 191, p. 9.

<sup>198</sup> LIBE draft report 2013, p. 63, 211.

<sup>199</sup> Chester 2012.

otherwise a cloud provider working in a specific sector (e.g. the medical sector) will have the legal uncertainty which national sectoral laws will apply to his services.<sup>200</sup>

One can conclude that the territorial scope is clearer because the equipment concept of the current Data Protection Directive is abandoned. However, the concepts of ‘offering goods and services’ and ‘monitoring the individual’ still have some room of interpretation and consequently create uncertainty for international operating cloud businesses if their products fall into the scope of the proposed Regulation. To prevent the situation of different interpretations by different stakeholders, the Commission should further specify these concepts, for instance in a recital.<sup>201</sup>

### 3.4 CONTROLLERS AND PROCESSORS

The commission sticks to the concepts of data controller and processor that have been introduced by the Data Protection Directive. The definition of the data controller is hardly changed; instead of determining the means and purposes of the processing, it is changed to the means, *conditions* and purposes. The concept of the data processor is defined in the same way as in the current directive.

The choice of keeping the concepts of a controller and processor almost the same is odd, outdated and conflicts with the aim to have a technology neutral Regulation. As discussed in chapter two, the concepts of controller and processor are outdated, especially in the context of cloud computing. It is often not clear which party is the controller and which the processor, because of the multitude of parties, complex technological structure and mixed resources. Furthermore, in some cases the cloud computing provider will claim to be neither a controller nor a processor, but just a facilitator.

Despite the fact that the concept of the controller is not changed much, the legislator strengthens the responsibilities to comply with the Regulation and to demonstrate this compliance, by introducing the principle of accountability in the Regulation.<sup>202</sup> This principle is well known<sup>203</sup> in the data protection debate and for the first time codified in European data protection law, in article 22 of the proposed Regulation to be exact.<sup>204</sup> In paragraph two of article 22, the legislator listed a non-exhaustive list of responsibilities of the controller and other chapters of the proposed Regulation oppose even more responsibilities and burdens, which will be discussed in the next paragraphs.

Recommended is to abandon the controller-processor-model because it is not sufficient anymore. An alternative is proposed by De Hert and Papakonstantinou in their article about the proposed regulation. They discuss the solution of letting the concept of processor go and “*vest the data controller title, rights and obligations upon anyone processing personal information, regardless of its means, conditions or purposes.*”<sup>205</sup> This will take away the legal uncertainty of data subjects and

---

<sup>200</sup> EDPS opinion 2012, p. 17.

<sup>201</sup> Kuner 2012, p. 6- 7; Blume 2012, p. 130 – 133; article 86 and recital 130 of the proposed Regulation.

<sup>202</sup> Proposed Regulation, p. 10; See also WP 173.

<sup>203</sup> EDPS opinion 2012, p. 27 – 29, WP 173, OECD Privacy guidelines, article 13

<<http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprivacyandtransborderfl oecdguidelineson.htm#part2>> last visited 30 January 2013.

<sup>204</sup> The word ‘accountability’ is not used in this article, probably because of the difficulties with the translating of the concept, see WP 173, p. 7 – 8.

<sup>205</sup> De Hert & Papakonstaninou, 2012, p. 133 – 134.

other stakeholders, but impose enormous burdens on cloud actors which sometimes are actually only a facilitator. Further in this chapter, it will be made clear that the burdens on the controller will only grow when the Regulation applies and imposing those burdens on processors as well will be very costly for them. The European legislator should to reconsider the choice of the obsolete model of the Data Protection Directive, while taking the cloud computing environment and the interests of all the stakeholders into account.

### 3.5 DATA SUBJECTS AND PERSONAL DATA

Conversely, there is a substantial change made to the definition of the data subject and his personal data. The definition of personal data is shortened to “*any information relating to a data subject*”<sup>206</sup>, which brings us to the definition of the data subject:

*'data subject' means an identified natural person or a natural person who can be identified, directly or indirectly, by means reasonably likely to be used by the controller or by any other natural or legal person, in particular by reference to an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;*<sup>207</sup>

This is a change with effects for cloud computing business, because of the online identifiers are explicitly recognized as personal data. Online identifiers are, among others, cookies and IP addresses and most of them are necessary for providing cloud services, for instance, to keep a user logged in. Noteworthy is recital 24 which states that the online identifiers “*need not necessarily be considered as personal data in all circumstances*”. Nevertheless, cloud computing companies should be aware that the digital information of their clients that they are using on a daily basis will probably fit the definition of personal data. Combined with the extended and clarified scope of the proposed Regulation, one can conclude that the influence of the European data protection legislation on cloud services is getting bigger.

The legislator failed (again) to touch upon the concepts of pseudonymous and anonymous data, which are very important in the context of data processing. Pseudonymisation and anonymisation techniques are techniques which will enhance the privacy of data subjects, without too much interference with the working of cloud computing services. The Commission should address these concepts and, even better, introduce alleviations for controllers and processors which uses these techniques. This will improve legal certainty, the protection of the personal data and the willingness of cloud providers to deploy their services in Europe<sup>208</sup>

### 3.6 CONSENT

The consent of the data subject is important for the lawfulness of the processing of personal data. The Data Protection Directive states that the consent “*shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data*

---

<sup>206</sup> Article 4 (2) of the proposed Regulation.

<sup>207</sup> Article 4 (1) of the proposed Regulation.

<sup>208</sup> MEP Albrecht encourages pseudonymisation and anonymisation in his report, LIBE draft report 2013, p. 5, 76 and 211, Hon et al. 2011 A.

*relating to him being processed.*"<sup>209</sup> Data processing is legitimate when the consent is unambiguously given by the data subject under the regime of the current Data Protection Directive.<sup>210</sup> The Commission drastically reinforced the concept of consent in the proposed Regulation. The legislator acknowledges the possibility of confusion by the terms of the current directive and introduces the requirement of *explicit* consent:

*'the data subject's consent' means any freely given specific, informed and explicit indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed;*<sup>211</sup>

Conditions for consent are given in article 7 of the proposed Regulation. The burden of proof always lies with the controller and the consent can be withdrawn by the data subject at any time. Furthermore, when consent is *"to be given in the context of a written declaration which also concerns another matter"*, the consent for the processing of personal data should be distinguishable from that other matter.<sup>212</sup>

Consent should therefore be a truly informed and explicitly given. It cannot be put away in privacy policies or general terms which a layman cannot understand, but has to be separated from the other matter. Consequently, the protection of the cloud end-user will rise by this introduction of explicitly given, truly informed consent. However, the burden on the cloud service providers will rise as well. If this approach survives the law making process, the cloud providers have to adopt the new consent requirement in their software and systems, a costly operation. Moreover, these stronger rules could also lead to burdens for cloud consumers, which will be prompted with pop-up's and more contracts, so the controller can be sure to really have the explicit consent of the data subject. An overload of consent request could lead to a 'consent fatigue' and will have a negative impact on the rights of the individual. A similar situation happened with the Dutch 'cookie law', which actually led to practical problems instead of a better protection of the rights of the citizens.<sup>213</sup>

A separate article regarding the processing of data of a child is created in the proposed Regulation. Article 8 states that if the data subject is below the age of 13 the consent has to be given or authorized by the subject's parent or custodian. One might think that it seems impossible to check whether a user of cloud services is a child or not without seeing it. The legislator therefore continues article 8 by stating that the controller should make *"reasonable efforts to obtain verifiable consent, taking into consideration available technology"*. The Commission will be empowered to specify criteria and requirements for this verifiable consent in delegated acts and lay down standard forms for specific methods to obtain such a verifiable consent.<sup>214</sup> Some cloud providers

---

<sup>209</sup> Article 2 (h) DPD.

<sup>210</sup> Article 7 (a) DPD.

<sup>211</sup> Article 4 (8) of the proposed Regulation.

<sup>212</sup> Article 7 (2) of the proposed Regulation.

<sup>213</sup> 'The Cookie Conundrum', available at <<http://leidenlawblog.nl/articles/the-dutch-cookie-conundrum>>, last visited 30 January 2013.

<sup>214</sup> Article 8 (3) jo. Article 86 of the proposed Regulation and Article 8 (4) jo. Article 87 (2) of the proposed Regulation.

already have age requirements of 13 and older<sup>215</sup>, but it is unclear how far they should go to check if their users really are above the minimum age. The verifying process could lead to a lot more data processing, for instance the obligation to send one's ID card, which is an undesirable development. The legislator had foreseen this development, with article 10 as the result. This article states that a controller does not have to identify a data subject if he is not permitted to do so, purely to comply with the Regulation.<sup>216</sup> It is not public yet what the definition of 'reasonable efforts' and 'verifiable consent' will be, and the Commission should be careful with these requirements, because they can impose a tremendous burden on cloud providers. After all, the actions of children are primarily the responsibility of their parents/custodians (e.g. installing parental control software) and not of cloud service providers.

### 3.7 RIGHT TO BE FORGOTTEN

An already heavily debated<sup>217</sup> article of the proposed Regulation is article 17. This article introduces the right to be forgotten<sup>218</sup>:

*Article 17 - Right to be forgotten and to erasure*

*1. The data subject shall have the right to obtain from the controller the erasure of personal data relating to them and the abstention from further dissemination of such data, especially in relation to personal data which are made available by the data subject while he or she was a child, where one of the following grounds applies:*

*(a) the data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;*

*(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or when the storage period consented to has expired, and where there is no other legal ground for the processing of the data;*

*(c) the data subject objects to the processing of personal data pursuant to Article 19;*

*(d) the processing of the data does not comply with this Regulation for other reasons.*

*(...)*

---

<sup>215</sup> Age requirements on Google Accounts, which are used for several SaaS services <<http://support.google.com/accounts/bin/answer.py?hl=en&answer=1350409>> last visited 30 January 2013 and Age requirement on Facebook <<https://www.facebook.com/help/210644045634222/>> last visited 30 January 2013.

<sup>216</sup> Albrecht suggested adding the line "The methods to obtain verifiable consent shall not lead to the further processing of personal data which would otherwise not be necessary." to article 8 (1), LIBE draft report 2013, p. 78 – 79.

<sup>217</sup> Rosen 2012; Sartor 2013; Kuner 2012 p. 11.; <<http://peterfleischer.blogspot.nl/2011/03/foggy-thinking-about-right-to-oblivion.html>> last visited 30 January 2013; EDPS opinion 2012, p. 24 – 25; WP 191, p. 13 – 14.

<sup>218</sup> The right to be forgotten has its roots in French law, criminals have 'the right of oblivion' (le droit à oubli), "a right that allows a convicted criminal who has served his time and been rehabilitated to object to the publication of the facts of his conviction and incarceration.", Rosen 2012 p. 88.

To discuss the consequences of this right to the cloud computing business, this paragraph distinguishes two situations. The first one is where the data subject himself puts personal data relating to him on a service (e.g. a social network site) of the cloud provider. The other situation is where the personal information of the data subject is uploaded on the same service *but* by another person.<sup>219</sup>

The right to be forgotten in the first situation is the least controversial. When the data subject uploads his own material, he has the right to take it down according to article 17. Most social network sites (Twitter, Facebook, and Google Plus) already allow users to take down their own uploaded content which seems only logical.

Far more controversial is the second situation. A short example: The data subject uploads a picture of himself on a social network site (SaaS) and takes it down after a while because he thought the picture was a bit embarrassing. The social network site deletes the picture; friends of the data subject however, copied and shared the picture on the same cloud service before the provider was able to erase the picture.

The first question one should ask is if the cloud provider is a controller. As can be read above and in the previous chapter, this is not an easy question. If the cloud provider is only a processor, the data subject has two options. Ask the friend (controller) to take the photo down and if necessary, threaten to sue or ask the cloud provider to take down the photo on the basis of the e-commerce directive. Because the social network provider probably will be a controller<sup>220</sup>, the next paragraphs will assume that the provider is so.<sup>221</sup>

In this case, the provider is obliged to delete the photo of the data subject which is copied on the same site by the friend. Cloud providers have to take down personal data of data subjects on their servers by request and if they refuse, they can risk enormous penalties. The fine of not accepting such a request can be 1.000.000 euro's or even 2% of the annual worldwide income.<sup>222</sup> On top of that, the provider has to compensate the damage of the data subject.<sup>223</sup>

The consequence of the introduced right to be forgotten is the situation where cloud providers become data protection law enforcers. The risk of the high fines and damage compensation is a circumstance in which the cloud provider has no choice but to remove the material uploaded by users which is personal data of a data subject, when that subject invokes his right to be forgotten. The user which uploaded the material has no right of objection or resistance on the basis of the proposed regulation. The implications of article 17 sub 1 are not clear, but one can conclude that it

---

<sup>219</sup> Sartor 2013 p. 9 and Rosen 2012 p. 89 – 90.

<sup>220</sup> The social network site can be considered to be a controller because it probably will determine the means, conditions and purposes of some of the processing of the personal data, WP 163.

<sup>221</sup> For more info about the situation when the provider is a processor, see Sartor 2013 p. 9 – 10.

<sup>222</sup> Article 79(5)(c) and 79(6)(c) of the proposed Regulation. To put it in perspective, Google's revenue of 2011 was 37.9 billion dollars, which could lead to a maximum fine of 758 million dollars <<http://investor.google.com/financial/2011/tables.html>> last visited 30 January 2013.

<sup>223</sup> Article 77 of the proposed Regulation.



could lead to a serious infringement of the rights of the internet-users and more specific, an unacceptable limitation of the freedom of expression.<sup>224</sup>

The implications of sub 2 of article 17 are also far from clear. The second paragraph of the right to be forgotten article places a heavy burden on data controllers and introduces a huge uncertainty on how to comply with it. The second paragraph of article 17 states the following:

*2. Where the controller referred to in paragraph 1 has made the personal data public, it shall take all reasonable steps, including technical measures, in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data. Where the controller has authorised a third party publication of personal data, the controller shall be considered responsible for that publication.*

Continuing the example of the friend of the data subject who uploaded a photo of that subject, this paragraph will discuss sub 2 of article 17. The uploaded picture can be copied by more friends and other internet users and placed on other cloud services (*inter alia* social network sites or forums). The controller of the data should then take all the reasonable steps to inform the users which copied that picture. When the cloud provider of the social network site where the friend of the data subject put the photo on is considered to be the controller, he has far going obligations to start an intensive internet search to find the copies of the photo. He has to inform all the third parties (which are probably cloud providers too) and ask them to take down the photo, with the same consequences as discussed above. This could place a huge burden on the cloud provider, which even becomes immeasurable when the photo has gone viral. It is unclear what the commission intends with 'reasonable steps', hopefully the delegated act further specifying this will not make the burden impossible high for the cloud providers. The Commission should take the technical possibilities into account; to comply with the second paragraph of article 17, cloud providers have to design complex web crawlers to find the data that is linked, copied or replicated by other parties and also the contact information of those parties. In combination with the reality of the internet and the massive transfer of data that is occurring these days, this seems to be an impossible operation and would definitely deter cloud providers to operate in the European Union. A possible solution one could think of is a notice on the webpage where the original data was, stating that the data is deleted and the strong advice to delete copies of and links to the data.

In article 17 (3), the legislator listed five exceptions to the right to be forgotten. The controller does not have to erase the data when the retention of the data is necessary for (a) exercising the right of freedom of expression<sup>225</sup>, (b) for reasons of public interest in the area of public health<sup>226</sup>, (c) for historical, statistical and scientific research purposes<sup>227</sup>, (d) for compliance with a legal obligation to retain the personal data by Union or Member State law<sup>228</sup> or (e) cases listed in sub 4 of article 17.

---

<sup>224</sup> Sartor 2013, p. 10 – 11. Rosen 2012, 88 – 92.

<sup>225</sup> Article 80 of the proposed Regulation.

<sup>226</sup> Article 81 of the proposed Regulation.

<sup>227</sup> Article 83 of the proposed Regulation.

<sup>228</sup> Full text of sub d of article 17 (3): “For compliance with a legal obligation to retain the personal data by Union or Member State law to which the controller is subject; Member State laws shall meet an objective of

At first sight article (17)(3)(a) might seem a valid protection of the freedom of expression, however, the legislator chose to appoint the controller to decide if the retention of the data is necessary for exercising the right of freedom of expression. It is incorrect to attribute such a legal task to a commercial party. First of all, the party will not be able to make the right decisions and will probably choose the cheapest option. Taken the severe penalties into account, this option will most likely be the choice of erasure. Secondly, the task will be a burden on the controller, a burden which should actually be placed on the courts (or the supervisory authorities).

Article 17's right to be forgotten is a controversial right which will put an enormous burden on cloud computing providers when applied strictly. Even worse is the chilling effect on the freedom of expression; the risk of high penalties will give the incentive to accept all erasure requests from data subjects and consequently, the right to be forgotten will transform in a right to censure.<sup>229</sup> Data protection law should never prevail over the freedom of expression. Therefore, to prevent the detriment of cloud providers in Europe, it is recommended to go back a few steps and only give data subjects the right to erasure personal data when it is inaccurate, incomplete, illegal, the processing is not in line with the rules of the proposed Regulation or, only for future processing, the subject withdraws its consent. Thus, stick to the regime of article 12(b), possibly accompanied with strong penalties which will be more legitimate in that case. When this recommendation cannot be fulfilled, the Commission should at least give more clarity regarding the scope of the right to be forgotten, because the right as it stands now, is far from clear, unrealistic and illegitimate<sup>230</sup>, in conflict with the 'reality how internet works'<sup>231</sup> and consequently creates a huge uncertainty for all the stakeholders.

### 3.8 RIGHT TO DATA PORTABILITY

The right to data portability is a new right which does not exist in the current Data Protection Directive or in other EU law.<sup>232</sup> The right of data portability gives the data subject the right to move his personal data from one controller to another, for instance, from Facebook to Google Plus<sup>233</sup>, when the data is provided and processed on the basis of consent or a contract. For cloud services, the subject's consent or contracts are the common ways to obtain data and therefore, the right to data portability will be applicable to the most services in the cloud computing business.

When a data subjects requests its data, Facebook should then, on the basis of article 16 of the proposed Regulation, send him his data in "*an electronic and structured format which is commonly used and allows for further use by the data subject.*"<sup>234</sup> Sub 2 of article 18 obliges the cloud provider

---

*public interest, respect the essence of the right to the protection of personal data and be proportionate to the legitimate aim pursued."*

<sup>229</sup> Sartor 2013 and Rosen 2012.

<sup>230</sup> LIBE draft report 2013, p. 98.

<sup>231</sup> WP 191, p. 13 – 14.

<sup>232</sup> "Only occasionally a requirement for automated data processing systems to be able to seamlessly cooperate among them is met, either in regulatory texts or through actions of the commission." De Hert & Papakonstaninou, 2012, p. 137.

<sup>233</sup> Not an unusual example, the right to data portability seems to aim at SaaS providers, Swire & Lagos 2012.

<sup>234</sup> Article 18 (1) of the proposed Regulation.

to give the data subject the possibility to transfer his data or other cloud service, “*without hindrance*”.

The right to data portability is introduced by the European Commission to improve the ability of the data subject to control his own data.<sup>235</sup> Data portability will solve the vendor lock-in problems<sup>236</sup> which lead to data protection risks in the cloud computing business.<sup>237</sup> Data interoperability is an interesting concept which contributes to standardization of technologies and therefore the technological development. In practice, many cloud providers, more specific SaaS providers, have a positive attitude to data portability.<sup>238</sup>

However, there are some strong concerns with article 18 of the proposed Regulation. Firstly, the burden that this article will impose on cloud providers will be very high, especially because the rules not only demand export possibilities but also data import mechanisms. The costs to adapt their services to provide such a high level of interoperability will be substantial, especially because the transfer should go ‘without hindrance’.

Secondly, while the proposed Regulation should *protect* the data of the individual, with the right of data portability, it creates an easy way to commit identity fraud because one can download a lifetime of data with just a few clicks.<sup>239</sup>

Finally, one might think this is more a matter of competition, and, in the field of competition law, it is not working. Peter Swire and Yianni Lagos conclude the same in their essay:

*“As a matter of competition law, Article 18 is over-broad, applying to small enterprises, and even when there is no monopoly power and no barriers to entry. Article 18 more generally is in conflict with the rules in competition law about exclusionary conduct – it creates a per se prohibition where competition would apply a rule of reason approach, considering efficiencies as well as possible harm to competition.”*<sup>240</sup>

The right to data portability will solve the vendor-lock in problems and gives the data subject more control over their data. However, the concept will create a heavy burden on the cloud providers to adapt their services. The costs of creating a module to export and import data will be high and consumers will be charged for that in the end. Furthermore, the protection of the personal data will not be enhanced. On the contrary, identity theft will be made much easier because downloading a lifetime of data will be done in a few clicks. On top of that one might ask if this is a data protection question at all. If it is a matter of competition law, then it fails in that way as well. Therefore, the European Legislator should erase the right to portability in this form from the Regulation. The

---

<sup>235</sup> EC communication 2012 A, p. 6.

<sup>236</sup> See chapter 2, para 2.2.2.2.

<sup>237</sup> WP 196, p. 5 – 7.

<sup>238</sup> Facebook: <<https://www.facebook.com/help/131112897028467/>> last visited 30 January 2013; Twitter: <<http://bits.blogs.nytimes.com/2012/07/24/twitter-is-working-on-a-way-to-retrieve-your-old-tweets/>> last visited 30 January 2013 Google: <<https://www.google.com/takeout/>> last visited 30 January 2013.

<sup>239</sup> Swire & Lagos 2012, p. 4 – 5.

<sup>240</sup> Swire & Lagos 2012, p. 45. See Swire & Lagos 2012, p. 14 – 31 for a more extensive opinion on article 18 of the proposed regulation in the perspective of competition law.

European Union could, however, encourage data portability via soft law and/or investments in open standards.

### 3.9 RIGHT TO OBJECT

The new article on the right to object (article 19 of the proposed Regulation) shifts the burden of proof of this right; the controller has to prove the data subject wrong when he refuses to accept the request of the data subject. This will further increase the burden on the cloud providers. Moreover, the wordings of article 19 of the proposed Regulation are unclear. The Commission should at least clarify the concept of ‘compelling legitimate grounds’ in a recital, because this concept was already unclear in the directive and now is the time to solve this.<sup>241</sup> Furthermore, the third paragraph states that “*Where an objection is upheld pursuant to paragraphs 1 and 2, the controller shall no longer use or otherwise process the personal data concerned.*” The definition of ‘upheld’ is unknown and, as mentioned by the EDPS, there is no explicit rule about what to do with the data when the controller and subject have a disagreement and no decision by e.g. a data supervisory authority is given. The relation between article 17 and 19 is thus unclear and the Commission should solve this and should clarify the concepts ‘compelling legitimate grounds’ and ‘upheld’.

### 3.10 PROFILING

The data subject has the right not to be profiled. The definition of profiling based on article 15 (1) of the Data Protection Directive and the Recommendation on Profiling by the Council of Europe<sup>242</sup>, is given in article 20 (1) of the proposed Regulation:

*A measure which produces legal effects concerning [a] natural person or significantly affects [a] natural person, and which is based solely on automated processing intended to evaluate certain personal aspects relating to this natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behaviour.*<sup>243</sup>

Because mining data of subjects is getting easier due the technological developments, profiling techniques are more and more used; cloud computing businesses play a big part in this. Individuals will get targeted advertisements on for instance cloud services or get a credit rating based on the profile made by the bank. Profiles are needed to make the overload of data manageable, but create privacy and data protection risks as well, such as the risk of unreliable or discriminatory profiles. Therefore, the European legislator created article 20, imposing strong restrictions on cloud providers who use profiling techniques. The second paragraph of article 20 gives the exemptions to the right not to be profiled. Individuals may be subjected to profiling techniques, when these are carried out in the course of entering in/performance of a contract, when these are expressly authorized by Member State of Union law or when the data subject has given his consent (article 7).

Welcoming the regulation of profile techniques to protect individuals’ rights, one should however note the problems with article 20. The ambiguous terminology of this article will lead to legal

---

<sup>241</sup> Schreurs et al. 2008, p. 251, Bainbridge 1997, p. 30.

<sup>242</sup> CoE Recommendation 2010.

<sup>243</sup> Article 20 (1) of the proposed Regulation, p 3.

uncertainty because the implementation in practice is unclear; the Commission should adjust the wordings of the article to take this uncertainty away.<sup>244</sup> Also, the delegated act “*further specifying the criteria and conditions for suitable measures to safeguard the data subject's legitimate interests*” should be adopted before the Regulation applies, for the sake of legal certainty.

Furthermore, the wordings of article 20 will possibly lead to a situation which is cumbersome for the cloud providers as well as the cloud consumers. Nowadays, many cloud providers are able to provide their services free of charge because of the revenue made by targeted advertisements. These targeted advertisements will probably fall into the scope of article 20 and therefore, to keep the services free, cloud services and websites using them are going to ask the individual for consent (or to enter in a contract). As a consequence, the cloud user will be exposed to consent pop-ups when using cloud services and because of the massive use of advertisements on the internet, the browsing experience will be lowered. Moreover, the overload of pop-ups will lead to a ‘pop-up fatigue’ and this will not contribute to the enhancement of the rights of individuals. The same with the possibility of ‘consent fatigue’, a situation like the Dutch cookie law must be avoided.<sup>245</sup> The Commission should take the reality of the internet as we know it (and the financing of it) into account when further specifying article 20, to prevent that problems similar to the Dutch cookie law case will rise.

### 3.11 DATA PROTECTION BY DESIGN AND BY DEFAULT

The principle of data protection by design is a concept where the controller is bound to meet the requirements of the Regulation by implementing “*appropriate technical and organizational measures and procedures*” at the first phase of the processing, i.e. “*at the time of the determination of the means.*”<sup>246</sup> A welcome principle in the world of cloud computing and especially because “*the state of the art and the cost of implementation*”<sup>247</sup> has to be taken into account, which makes the burden on the cloud providers proportional.

The other principle of article 23, data protection by default, is less clear. Especially the meaning of ‘default’ is ambiguous.<sup>248</sup> In all likelihood it will mean that the most privacy friendly settings should be turned on by default<sup>249</sup>, which is not always the best option. For instance, many cloud services are used for public communication and sharing (personal) data, the most privacy friendly setting will be “*contrary to the fundamental nature of the services and to how most users would wish to use them.*”<sup>250</sup> Furthermore, this principle does not always add that much to the general principles of the proposed Regulation, specifically the data minimization principle.<sup>251</sup> Taking into account the

---

<sup>244</sup> Kuner 2012, p. 11.

<sup>245</sup> ‘The Cookie Conundrum’, available at <<http://leidenlawblog.nl/articles/the-dutch-cookie-conundrum>>, last visited 30 January 2013.

<sup>246</sup> Article 23 (1) of the proposed Regulation.

<sup>247</sup> Article 23 (1) of the proposed Regulation.

<sup>248</sup> EDPS opinion 2012, p. 29 – 30, Kuner 2012, p. 12 – 13.

<sup>249</sup> Reding 2012, p. 126, Kuner gives the following example: “*e.g., that certain [privacy] settings in Internet browsers are turned on from the time the browser is first used*” Kuner 2012, p. 13.

<sup>250</sup> CDT Analysis 2012, p. 7.

<sup>251</sup> General principles are found in article 5 of the proposed Regulation, the data minimization principle is codified in sub c of that article.

unclearness of this principle, the fact that it is sometimes unnecessary and the possible conflict with the preferences of the user and the nature of the service, the Commission should delete the data protection by default principle from the Regulation. The legislator could implement a provision which obliges the cloud provider to give simple and unambiguous privacy options to its users, including a ‘most privacy friendly’ option. That way, the same result will be achieved, without the disadvantages mentioned above.

### 3.12 REPRESENTATIVES

Article 25 obliges controllers to designate a representative in the situation described in article 3 (2)<sup>252</sup>. The representative may be addressed by all the stakeholders with regard to the obligations following from the proposed Regulation<sup>253</sup>, such as the data subjects themselves<sup>254</sup> and the supervisory authority.<sup>255</sup> This is an improvement of the rules regarding representatives in the Data Protection Directive, which had some practical problems.<sup>256</sup> Article 25 continues with some exemptions, some obvious, such as small companies and public bodies, some controversial, such as controllers established in third countries recognized as providing adequate protection. The Commission should take the recommendation of the European Data Protection Supervisor into account; his advice is to delete this exemption, for the sake of enforcement.<sup>257</sup> As can be read in chapter two, it is hard to enforce the data protection legislation when the controller is not established in a Member state, obliging the controller to designate a representative improves the possibility for data subjects to invoke their rights and the possibility to impose penalties.<sup>258</sup> This will boost the rights of the individuals and the legal certainty of companies and consumers. Boosting those rights will in turn strengthen the incentive to use cloud computing services.

### 3.13 DOCUMENTATION

Controllers have an obligation to notify the supervisory authority in each case of processing of personal data in the current Data Protection Directive. Obviously that is an unworkable situation in the field of cloud computing and an example of the fact that the directive is outdated.<sup>259</sup> Luckily the Commission revised this obligation of notification with the new article 28 of the proposed Regulation. This article obliges the controller to “*maintain documentation of all processing operations under its responsibility*”<sup>260</sup> and to “*make [this] documentation available, on request, to the*

---

<sup>252</sup> Article 3(2) of the proposed Regulation: *This Regulation applies to the processing of personal data of data subjects residing in the Union by a controller not established in the Union, where the processing activities are related to:*

*(a) the offering of goods or services to such data subjects in the Union; or*

*(b) the monitoring of their behaviour.*

<sup>253</sup> Article 4 (14) of the proposed Regulation.

<sup>254</sup> Article 14 (1) (a) of the proposed Regulation.

<sup>255</sup> Article 28 (3) and 29 of the proposed Regulation.

<sup>256</sup> See chapter 2, para 2.2.3.3, also acknowledged by the Article 29 Working Party, see WP 179, p. 23.

<sup>257</sup> EDPS opinion 2012, p. 30.

<sup>258</sup> The representative is liable for the penalties which can be initiated on the controller, article 78 (2). Kuner 2012, p. 13.

<sup>259</sup> One should note that many Member states used the possibility for exemptions and simplifications of the obligation to notify, EDPS opinion 2012, p. 31.

<sup>260</sup> Article 28 (1) of the proposed Regulation.

*supervisory authority.*<sup>261</sup> The contents of the documentation are regulated in the second paragraph of the new article.

*The documentation shall contain at least the following information:*

*(a) the name and contact details of the controller, or any joint controller or processor, and of the representative, if any;*

*(b) the name and contact details of the data protection officer, if any;*

*(c) the purposes of the processing, including the legitimate interests pursued by the controller where the processing is based on point (f) of Article 6(1);*

*(d) a description of categories of data subjects and of the categories of personal data relating to them;*

*(e) the recipients or categories of recipients of the personal data, including the controllers to whom personal data are disclosed for the legitimate interest pursued by them;*

*(f) where applicable, transfers of data to a third country or an international organisation, including the identification of that third country or international organisation and, in case of transfers referred to in point (h) of Article 44(1), the documentation of appropriate safeguards;*

*(g) a general indication of the time limits for erasure of the different categories of data;*

*(h) the description of the mechanisms referred to in Article 22(3).*

Eliminating the obligation to notify from the new rules is a welcome decision, but the new article is not a good solution to fill the empty space of the deletion. The administrative burden of documenting all the processing operations is too high for a cloud provider and in conflict with the objective to reduce the administrative burden. Companies in the cloud computing business should implement costly software to monitor their processing in the way demanded by the proposed Regulation.<sup>262</sup> Furthermore, the goal of the article, documentation of processing activities and the compliance with the data protection rules during this activities, can be fulfilled with less requirements. Following the opinion of the European Data Protection Supervisor, the Commission should simplify this article by keeping a documentation of the processing operations containing only the demands of sub a, b and h of article 28 (1) “*with a duty to keep an inventory of all processing operations for which the controller is responsible as well as a description of the way in which the controller has ensured that these processing operations comply with data protection rules.*”<sup>263</sup> That way the purpose of article 28 is maintained and the burden is much lower because of the erasure of sub c, d, e, f and g. This seems to be the best solution in finding the equilibrium of the right of data protection and commercial interests.<sup>264</sup>

---

<sup>261</sup> Article 28 (3) of the proposed Regulation.

<sup>262</sup> Which can be further specified by the commission, article 28 (5) and (6) jo. Article 86 and 87 (1) of the proposed Regulation.

<sup>263</sup> EDPS opinion 2012, p. 31.

<sup>264</sup> EDPS opinion 2012, p. 30 – 31.

### 3.14 DATA BREACH NOTIFICATION

Article 31 and 32 of the proposed Regulation obliges the controller to notify the supervisory authority and data subjects in the case of a data breach. Data breach notification is not a new subject and already exists, for instance, in article 4 of the e-privacy directive, Australian and U.S. law.<sup>265</sup> The Commission defines the concept of a data breach in the proposed Regulation<sup>266</sup>, but fails to further specify when such a breach is established and when exactly the Data Protection Authority and data subject should be notified.<sup>267</sup> It should be stressed that the threshold of a breach is very important for the effectiveness of article 31 and 32. When it is too high, data subjects will not be informed when their data is breached, with all the consequences. On the other hand, when the criteria are not strict enough, people will receive lots of notifications and this will cause a so-called 'notification fatigue', as acknowledged by the Commission.<sup>268</sup> The commission is empowered to adopt delegated acts regarding these concepts, but for the sake of legal certainty it should add the specification to the Regulation (in article 31/32 or recitals) or at least make sure to adopt the delegated acts at the moment when the Regulation takes legal effect.

Moreover, the deadline of notification set in the article 31 is unrealistic and undesirable in practice; Paragraph 1 of this article states that the supervisor has to be notified no later than 24 hours, which is too short. The legislator added "*where feasible*" to the sentence to permit delay, but with the requirement of a "*reasoned justification*". 24 Hours is not a realistic deadline and will not work in practice,<sup>269</sup> as stated by the Commission in its impact assessment: "*A 'quick and dirty' notification rushed out to meet a deadline, which then requires updates and corrections will cause more insecurity concern and loss of confidence of data subjects than it provides benefits to users.*"<sup>270</sup> To prevent such rushed notifications and improve the effectiveness the deadline should be changed to 72 or 96 hours.<sup>271</sup>

### 3.15 DATA PROTECTION OFFICER

The obligation to designate a Data Protection Officer (DPO) can be found in article 35 and its position and tasks in respectively article 36 and 37. It is not a new concept but for the first time mandatory.<sup>272</sup>

Companies employing less than 250 employees are exempted from article 35<sup>273</sup>; some argue that the exemption for micro, small and medium enterprises (MSME'S) to designate a DPO should be

---

<sup>265</sup> See Pattison 2012 for Australian law and <<http://www.ncsl.org/issues-research/telecom/overview-security-breaches.aspx>> (last visited 30 January 2013) for the situation in the United States.

<sup>266</sup> Article 4 (9) of the proposed Regulation states "*'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;*".

<sup>267</sup> EDPS opinion 2012, p. 32.

<sup>268</sup> EC impact assessment, annex 6, p. 83.

<sup>269</sup> EDPS opinion 2012, p. 32, Kuner 2012, p. 14, , LIBE draft report 2013, p. 123 – 124, WP 191, p. 16 – 17.

<sup>270</sup> EC impact assessment, annex 6, p. 84.

<sup>271</sup> Kuner 2012, p. 13 – 14.

<sup>272</sup> The obligation of designating a DPO is already known in the Regulation (EC) No 45/2001, see article 24 of that regulation and also in some Member States, Kuner 2012, p. 15.

<sup>273</sup> Article 35 (1) (b) of the proposed Regulation.



lowered to an amount of employees less than 250.<sup>274</sup> It is true that in certain small countries, such as Austria, most companies will fall in the scope of the MSME's exemption, but they still have to designate a DPO if their core activities "*consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects*" on the basis of Article 35 (1) (c) of the proposed Regulation. This criterion needs some clarification to prevent legal uncertainty<sup>275</sup>, but will expand the scope of article 35 enough to have the MSME's exemption maintained, which is in favor of new cloud computing businesses entering the market.

Moreover, companies will probably designate a DPO by themselves, because the Data Protection legislation is getting more complicated and asks more from companies, a DPO is therefore useful. Especially because of the remedies and sanctions found in chapter 8 of the proposed Regulation, a DPO would be a good investment. Furthermore, the Data Protection Officer can be a part-time function<sup>276</sup> and a group of undertakings may appoint one single data protection officer.<sup>277</sup> For this reasons, the introduction of this obligation is welcome, but further specifying sub c of article 35 (1) is recommended.

### 3.16 TRANSFER TO THIRD COUNTRIES

The regime of the Data Protection Directive regarding third transfers is not practical in the light of cloud computing. As can be read in chapter two, the fourth chapter of the directive is limiting the free flow of information tremendously.<sup>278</sup> The transfer to third countries is an important subject for cloud computing stakeholders, because of the worldwide transfers and international environment of cloud computing services. The Commission revised the rules regarding transfers to third countries, with chapter five of the proposed Regulation as result.

The Commission let go of the requirement ensuring an 'adequate level of protection' by the third country and replaced it with the requirement with the general principle that the conditions of the proposed Regulation should be met, also for onward transfers, an important detail for cloud providers. Chapter five continues with three mechanisms to legalize the transfer to specific third countries, these mechanisms will be discussed below.

#### 3.16.1 TRANSFERS WITH AN ADEQUACY DECISION

The legislator continues the possibility to issue adequacy findings and codifies this in article 41 of the proposed Regulation. Changes with the rules of the current Directive are *inter alia* the possibility to decide that "*a territory or a processing sector within that third country, or an international organisation ensures an adequate level*".<sup>279</sup> The commission can also decide to find a third country (or territory/sector/organization) not adequate and transfer to them will be prohibited.<sup>280</sup> An exemption to this prohibition can be found in paragraph 6 of article 41: "*without*

---

<sup>274</sup> This is, for instance, the opinion of the Data Protection Supervisor, see EDPS opinion 2012, p. 34.

<sup>275</sup> EDPS opinion 2012, p. 34.

<sup>276</sup> One should note that other professional activities of the DPO may not be in conflict with the tasks and duties of the officer, article 35 (6) of the proposed Regulation.

<sup>277</sup> Article 35 (2) of the proposed Regulation.

<sup>278</sup> Chapter 2, para 2.2.4 and 2.2.5.

<sup>279</sup> Article 41 (3) of the Proposed Regulation.

<sup>280</sup> Article 41 (5) and (6) of the Proposed Regulation.

*prejudice to Articles 42 to 44*".<sup>281</sup> A welcome exemption, which is oddly contradicted with the accompanying recital 82. The Commission should set this contradiction straight, in such a way that transfers to a third country which is not adequate are still possible under circumstances.<sup>282</sup>

Despite these changes, one can state that the regime of adequacy decisions is not changed substantially. This is an unwanted situation; the adequacy decision procedure is a lengthy process and could use a reform. It is not a coincidence that there are not many adequacy decisions given by the Commission.<sup>283</sup> The Commission should take the opportunity to reform the decision procedure as well, to enhance the effectiveness of article 41 of the proposed Regulation.

### *3.16.2 TRANSFERS BY WAY OF APPROPRIATE SAFEGUARDS*

If there is no adequacy decision given by the Commission for a certain third country, transfer of data is still possible when the controller or processor "*has adduced appropriate safeguards with respect to the protection of personal data in a legally binding instrument*."<sup>284</sup> The following mechanisms are listed in article 42 (2): (a) Binding Corporate Rules, (b) standard data protection clauses adopted by the Commission, (c) standard data protection clauses adopted by a supervisory authority and (d) contractual clauses between the controller or processor and the recipient of the data authorized by a supervisory authority. The mechanisms in sub a, b and c do not need any authorization. Consequently, the requirement of authorization of standard contractual clauses is deleted and this will be applauded by the cloud computing businesses.<sup>285</sup>

#### **3.16.2.1 Binding Corporate Rules**

The legislator codified the mechanism of Binding Corporate Rules (BCR's)<sup>286</sup> in the text of the proposed Regulation, more specific article 43. The codification should be welcomed by the cloud computing providers because 'remaining legal barriers' on the use of BCR's are finally removed. The Commission sticks to the text of Article 29 Working Party on BCR's<sup>287</sup> and with success; especially the applicability for processors is received gladly. <sup>288</sup>

### *3.16.3 EXISTING DECISIONS AND MECHANISMS*

As stated above, the Commission has not released many adequacy decisions.<sup>289</sup> However, the agreements and standard contractual clauses with third countries which are in force are very important. Essential countries in the cloud business, such as Canada, United States and Australia,

---

<sup>281</sup> Article 42 'Transfers by way of appropriate safeguards' and 44 'Derogations' will be discussed in the next paragraphs.

<sup>282</sup> EDPS opinion 2012, p. 36.

<sup>283</sup> Chapter 2, para 2.2.4; Kuner 2012, p. 16; states which have obtained such an adequacy finding can be found at <[http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm)> last visited 30 January 2013.

<sup>284</sup> Article 42 (1) of the proposed Regulation.

<sup>285</sup> Kuner 2012, p. 17.

<sup>286</sup> For more information regarding BCR's, see Moerel 2011 B.

<sup>287</sup> WP 153.

<sup>288</sup> Kuner 2012, p. 17.

<sup>289</sup> States which have obtained such a adequacy finding can be found at <[http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm)> last visited 30 January 2013.

have received positive decisions or frameworks<sup>290</sup> and transfers to these countries are allowed under the regime of the current Data Protection Directive. Article 41 (8), 42 (5), recital 79 and 134 confirm that decisions taken on the basis of the soon to be repealed directive stay in force. A welcome recital for cloud computing companies, because of many cross-border data transfers. In the case of the repealing of these decisions when the new data protection framework entries in force, a huge gap will come in existence and cloud businesses have to wait for new decisions, which will have a chilling effect on the cloud computing market.

However, in some cases, it is unclear how current the decisions and mechanisms interact with the proposed Regulation. The rules of the Regulation are stricter and therefore, the requirements of the transfer of data to third countries are stricter as well. For this reason, it is desirable that the decisions and mechanism that are currently in place should be replaced or amended in line with the proposed Regulation. Both the draft report from the European Parliament and the European Data Protection Supervisor vouch for a deadline of two years.<sup>291</sup> However, one should take into account the importance of such decisions and notice that amendments or replacements made in a hurry are not desirable. Well-considered and negotiated international agreements are needed to ensure the protection of the fundamental rights of individuals and boost the development of cloud computing in Europe. Thus, the recommendation to the Commission is to review the existing decisions and align them to the Regulation within 'a reasonable timeframe'.<sup>292</sup>

#### 3.16.4 DEROGATIONS

Article 44 of the proposed Regulation is the new version of article 26 DPD. A controversial change is sub h of paragraph 1 of the new article, which allows derogation when the transfer "*is necessary for the purposes of the legitimate interests pursued by the controller or the processor*". This provision is considered to be a 'loophole' by human rights activists, but will not be discussed further because the transfer should not be "frequent or massive" and therefore cloud services are excluded from the derogation.

#### 3.16.5 DISCLOSURES NOT AUTHORIZED BY UNION LAW

Chapter two touched upon the disclosures to non-EU agencies or courts and the Commission drafted a separate article for it in the interservice version of the proposed Regulation.<sup>293</sup> Unfortunately, the article and its five paragraphs did not survive the legislative process, only leaving recital 90: "*(...) The extraterritorial application of these laws, regulations and other legislative instruments may be in breach of international law and may impede the attainment of the protection of individuals guaranteed in the Union by this Regulation. Transfers should only be allowed where the conditions of this Regulation for a transfer to third countries are met (...)*".

For the sake of legal certainty and consequently a higher incentive to use cloud services by companies and individuals, the Commission should introduce a new article with the content of article 42 of the interservice version of the proposed Regulation, which is a suitable provision "to

---

<sup>290</sup> E.g. the safe harbor framework agreement in the case of the United States.

<sup>291</sup> LIBE draft report 2013, p. 150, 152, EDPS opinion 2012, p. 35.

<sup>292</sup> Kuner 2012, p. 17.

<sup>293</sup> Article 42 of the interservice version of the proposed Regulation.

*address the issue raised by access requests by public authorities or courts in third countries to personal data stored and processed in the EU*".<sup>294</sup>

### 3.17 SUPERVISORY AUTHORITIES

The regulatory patchwork created by the current Data Protection Directive has the consequence of a patchwork of supervisory authorities. The legislator tried to fix this patchwork and strengthen the independence of the authorities, the latter aligns with the ruling of the Court of Justice in the *Commission v Germany* case.<sup>295</sup>

The last sentence of the article 46 (1) of the proposed Regulation ("*the supervisory authorities shall co-operate with each other and the Commission*") and a separate chapter on the co-operation and consistency is proof of the will of the Commission to harmonize the role of the supervisory authorities. Of course, only practice will tell if this will work as desired by the legislator, but for now the intentions and the words of the two chapters will probably well received by the stakeholders of the cloud computing business, which will all benefit from the co-operation and consistency.<sup>296</sup>

#### 3.17.1 ONE-STOP-SHOP

The current 'competency on the territory of its own Member State' rule of the DPD<sup>297</sup> will be complemented by article 51 of the proposed Regulation, which provides a "*new competence as lead authority in case that a controller or processor is established in several Member States*".<sup>298</sup>

The 'main establishment' of the controller or processor is decisive for the determination of the leading authority.<sup>299</sup> The definition of the main establishment, which can be found in article 4 (13) of the proposed Regulation, is not entirely clear. Recital 27 is meant to clarify the concept, but contradicts itself, this should be clarified.<sup>300</sup>

The role of a lead authority constitutes also another problem; that of the possibility of an unfair contest between a cloud company and a lead authority. Christopher Kuner gives a perfect description of this problem: "*(...) a smaller and less-resourced [Data Protection Authority] in a member state where the company has its main establishment may become competent to supervise the company's activities all over the EU, which could place great pressure on its capacities and on cooperation with other [Data Protection Authorities]*".<sup>301</sup> A way to solve this is via the budget of the

---

<sup>294</sup> LIBE draft report 2013, p. 155 – 156.

<sup>295</sup> "As has already been stated, the independence of the supervisory authorities, in so far as they must be free from any external influence liable to have an effect on their decisions, is an essential element in light of the objectives of Directive 95/46. That independence is necessary in all the Member States in order to create an equal level of protection of personal data and thereby to contribute to the free movement of data, which is necessary for the establishment and functioning of the internal market.", CJEU Case C-518/07, *European Commission v Federal Republic of Germany*, [2010] ECR I-01885

<sup>296</sup> De Hert & Papakonstantinou, 2012, p. 138 – 139.

<sup>297</sup> Article 28 (6) DPD.

<sup>298</sup> Paragraph 3.4.6 of the Explanatory Memorandum of the proposed Regulation.

<sup>299</sup> Article 51 (2) of the proposed Regulation.

<sup>300</sup> Kuner 2012, p. 19. WP 191, p. 10 – 11, 18.

<sup>301</sup> Kuner 2012, p. 19.

authorities, which is a controversial subject itself.<sup>302</sup> When determining the formula for the budget of a supervisory authority, an element of the number of headquarters of multinational corporations established in a Member State can be taken into account and therefore the balance between the authority and multinational entity will be restored.<sup>303</sup>

Moreover, there is no clear rule on which supervisory authority is the leading one when the controller or processor is not established in a Member State, but the Regulation still applies on the basis of article 3 (2). The Working Party lists suitable proposals of criteria for determining the lead authority. Such as choosing the supervisory authority of the Member State (1) *“in which the main processing activities in question are taking place”*, (2) *“in which individuals are affected”* or (3) *“in which individuals have specifically complained to or raised concerns with the [data protection authority], according to article 73 (1)”*.<sup>304</sup> In the case where several authorities fulfill the criteria, they should *“agree amongst themselves who should take on the responsibility of being lead”*.<sup>305</sup>

The one-stop-shop provision of the proposed Regulation will be of great benefit to the cloud providers and other actors in the cloud computing business. However, the definition of a ‘main establishment’ should be clarified and the legislator should take care of the possibility of inequality between a multinational and the leading authority, for instance by taking this into account while reviewing the budget provisions. Furthermore, the legislator should fill the gap of the leading authority when the controller is not established in the Union, for instance based on the criteria proposed by the Working Party.

### 3.18 CONCLUSION

More than fifteen years after the adoption of the Data Protection Directive the European legislator has published a proposal for a General Data Protection Regulation. This chapter analyzed the proposed Regulation and discussed if the shortcomings of the DPD in the light of cloud computing are solved in this new piece of legislation, which, according to the Commission, is prepared for this technological complexity.

One of the ways the legislator tried to fix the regulatory patchwork of the current Directive is to propose a regulation. This chapter concluded that the choice for a regulation is a good one; the actual text however still creates a small patchwork, especially because of the 45 provisions which can be further specified by the Commission via delegated and implementing acts.

When analyzing the text, one will notice a lot of changes which will be applauded by the cloud computing stakeholders. For example, the notification obligation is deleted, the supervisory authorities will work co-operate (more) and there is a one-stop-shop for cloud providers. Also the concepts of personal data, consent and the territorial scope are more clarified, a welcome change.

---

<sup>302</sup> For practical reasons, the budget discussion will not be analyzed here, for more information regarding this subject, see EDPS opinion 2012, p. 18 en WP 191 p. 8 – 9, 17.

<sup>303</sup> This is a suggestion made by the Working party in the discussion regarding the budget, see WP 191, p. 17.

<sup>304</sup> WP 191, p. 19.

<sup>305</sup> WP 191, p. 18 – 19.

However, the proposed Regulation also included new rights which will put a tremendous burden on the controller. The principle of data protection by default, the right to be forgotten and the right to data portability are not suitable for the cloud computing environment. Also the rules regarding the notification breach and the documentation requirement are in the current wordings undesirable.

The rules regarding transfer to third countries, an important subject in the cloud computing sector, are improved, but the Commission failed to take the opportunity to really make a difference. The same applies to the controller-processor model, the moment to solve the issues with this model is now, but the legislator does not seem to have the answer.

## CONCLUSION

The publication of the reform package of Europe's data protection legislation triggered the choice of the subject of this thesis. Especially in a complex, technological environment as cloud computing, the effects of data protection rules are interesting. Therefore, this thesis discussed the effects of the European Data protection Directive and proposed Regulation, with the purpose to research if the proposed reform of the Data Protection framework contributes to the EU's ambition to become a world cloud computing powerhouse.

To answer this question, one should first know the definition of cloud computing. The first chapter reviewed several definitions and instead of adding another definition to the list it analyzed the actors, models and characteristics of cloud computing and their importance regarding data protection. It listed the essential actors in the cloud computing business (cloud provider, consumer and sometimes the aggregators) and explained the division made between private, public, community and hybrid cloud services. Furthermore, it analyzed the different service models; Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Examples of distinctive characteristics are virtualization, resource pooling, scalability and elasticity, which can lead to, among others, issues with transparency, transnational data flows and accountability concerns.

The technological development of the internet of the last decade, with cloud computing as one the results, should definitely be regulated by data protection legislation, however, the second chapter concluded that the current Data Protection Directive was not capable of fulfilling this mission. This chapter identified the problems of the - more than fifteen year old - directive and pinpointed the troubles it had with the characteristics of cloud computing. Firstly, the choice of instrument, a directive, has led to a regulatory patchwork in the European Union. Each Member State has its own (slightly different) laws and for international operating cloud computing providers it is almost impossible to comply with all of them. Also a Supervisory Authority in each state is contributing to aforementioned patchwork, especially because of the lack of co-operation.

Secondly, chapter two concludes that the controller-processor concept is outdated and not capable of dealing with the complex systems of cloud providers. In practice, the answer to the questions 'who is really in control' and 'who is qualified by the Directive as a controller' differs and sometimes it is very complicated to find the right controller for a specific processing activity in the cloud computing labyrinth.

Furthermore, the scope and applicability of the Data Protection Directive are in some cases unclear, mainly because of the ambiguous definitions of important concepts like 'personal data', 'establishment' and 'use of equipment'. Also the vagueness regarding encryption and anonymization is a disadvantage for cloud computing stakeholders.

More concerns rise on the rules regarding transfers to third countries, these rules provide tools for transferring personal data outside the EU, but these tools seem to be unsuitable for the massive flows of data of current times.

Therefore, the second chapter concludes that a reform of the Data Protection Directive is certainly desirable. As acknowledged by the EU itself, the current Directive is not sufficient in dealing with the modern issues created by the complex cloud computing systems.

The European Commission proposed, for this reason, a reform package which contains a General Data Protection Regulation and a Directive regulating the rules regarding judicial activities. The third chapter discussed if the reform could handle the several challenges set out in the first two chapters. It has its main focus on the proposed Regulation, because of its importance for cloud computing businesses.

After a short introduction on the background of the reform, the chapter discussed the choice for a regulation. One can conclude that this choice is the right one in the light of cloud computing, because of the direct effect in national law and therefore the diminishing effect on the patchwork created by the Directive. Every stakeholder in the cloud computing business will gain from the harmonized and comprehensive legislation in the field of data protection. However, there are some side notes that have to be made. First, the Member States will still have some room of maneuver under the regime of the Regulation. Secondly, other directives regulating E-Privacy, Data Retention, Judicial Activities and the Regulation for EU institutions, bodies and agencies could interfere with the desired harmonization. Finally, the Commission is empowered to adopt delegated and implementing acts, which can lead to a bulk of secondary legislation. To reduce the amount of extra legislation, the following advice is made in chapter three:

---

*The Commission should review all the articles where it gave itself the power to adopt delegated and implementing acts and reconsider if the powers are really necessary or even legal in the light of article 290 (1) TFEU.*

---

The chapter continued with the scope of the proposed Regulation. Minor changes were made to the material scope, which led to the maintaining of the criticized Household exemption. The Commission abandoned the difficult concept of 'the use of equipment', and introduced the new concepts of 'offering of goods and services' and 'monitoring', both could use more clarification.

---

*Data processors when providing a service to a natural person whose processing falls into the scope of the household exemption (article 2 (d)) should be bound by the same requirements as regular processors. The Commission should further specify the concepts of 'offering of goods' and 'monitoring'.*

---

The definition of personal data is substantial for the scope and applicability of the proposed Regulation. The Commission clarified the concept but fails to touch upon pseudonymisation and anonymisation techniques, which are widely used and favorable for the protection of personal data. For the sake of legal certainty, data protection and the digital market, the following advice is given:



---

*The Commission should touch upon the concept of pseudonymisation and anonymisation and introduce alleviations for controllers and processors which use these techniques*

---

Another criticized part of the current Directive that is maintained in the proposed Regulation is the controller-processor model. The increment of the burdens of cloud providers by the accountability principle that is associated with this model is discussed as well. In the second chapter the disadvantages of the use of the concepts of controller and processors and the last chapter gave, on the basis of these arguments, the following recommendation:

---

*The Commission should reconsider the choice of the obsolete controller-processor model, while taking the cloud computing environment and the interests of all the stakeholders into account.*

---

In paragraph five the changes to the concept of personal data are discussed and the conclusion is that the influence of the Data Protection legislation is growing larger, especially because of the extended and clarified scope. This is a welcome development for data subjects using cloud services.

The notion of 'consent' is strengthened as well, which will also lead to a higher burden on cloud providers. Regarding the new article 8 (Processing of personal data of a child), the advice below is made by arguing that the activities of a child on the internet are primarily the responsibility of the parents and one should take the difficulties of the process of verifying the age of a data subject into account.

---

*The Commission should be careful with the requirements for 'reasonable efforts' and 'verifiable consent' (article 8), because of the possibility of unrealistic tremendous burdens on cloud providers.*

---

An even higher burden on cloud providers is created by the heavily debated right to be forgotten. This right conflicts with the freedom of expression and is unrealistic in its current form given the current state of the internet. It will impose huge burdens on cloud providers and even ask them to act like law enforcers. Therefore, the following recommendation is given in the last chapter:

---

*At least clarify the scope of article 17 and even more desirable, reduce the scope considerably to the same scope of the already extensive rights of erasure in the Data Protection Directive.*

---

Chapter three also criticizes, in the light of the cloud computing, the new right to data portability. It states the advantages of data interoperability, such as standardization of technology and solution for the vendor-lock in problems, and underlines the positive attitude of most cloud providers to this concept. However, the burden created by article 16 on the cloud provider is disproportional, identity theft will be made easy and, most substantial, this is more of a matter of competition law. The erasure of this principle is desirable:

---

*The Commission should delete the Right to Data Portability in the form of the proposed article 16 from the Regulation*

---

The next subjects that are touched upon by chapter three are the rules regarding the right to object and profiling. The rising burden on cloud providers and the evolution of the internet as we know it are discussed and the following recommendations are given:

---

*The Commission should clarify the relation between article 17 and 19 and further specify the definitions of 'compelling legitimate grounds' and 'upheld'.*

---

---

*To prevent practical problems, the Commission should update and clarify article 20, taking the working of the internet into account.*

---

The principles of Data Protection by Design and by Default are respectively welcomed and rejected in this thesis. Data protection by design has positive effects for the cloud consumers and the burden on cloud providers is made proportional by the wordings of article 23 of the Proposed Regulation. This is the opposite of the principle of data protection by default, which is unclear in its current wordings and sometimes unnecessary. Moreover, it conflicts with the nature of the cloud service and the wishes of the user. Therefore, the following advice is given:

---

*The Commission should delete the Principle of Data Protection by Default (article 23 (2)).*

---

Subsequently, the rules regarding the designation of representatives are discussed. These rules will boost the rights of individuals and the legal certainty when using cloud computing services from a provider which is not established in a Member State. This will lead to a higher incentive for companies and consumers to use cloud services, and therefore article 25 is welcomed in the light of the cloud computing business. Also the mandatory designation of Data Protection Officer by large

companies is welcome, because of the complicated obligations of data protection laws and the possible high sanctions.

The articles regulating the documentation and data breach notification obligation will not be welcomed that much by the cloud computing providers. The documentation requirements are too high a burden on cloud service providers and should be reduced. Also the notification deadline should be reduced and furthermore, the rules regarding data breach notification should be further specified to prevent legal uncertainty.

---

*The Commission should reduce the requirements of documentation by deleting sub c, d, e, f and g of article 28 and instead introduce a duty to keep an inventory with all the processing operations combined with a description of the compliance with the rules of the Regulation.*

---

---

*The Commission should further specify the threshold of the data breach notification articles (31 and 32) in the Regulation or its recitals, or at least in implementing or delegated acts before the Regulation will entry in force. Furthermore the notification deadline should be expanded to 72 or 92 hours.*

---

One of the last subjects the third chapter touched upon is an important one: the transfer of personal data to third countries. The European legislator abandoned the concept of 'adequate level of protection' and replaced it with the requirement of meeting the conditions of the proposed Regulation. The three ways to legalize transfers to third countries are via adequacy decisions, appropriate safeguards and derogations. Regarding the first option it is noted that the Commission fails to review the decision procedure, which is complicated and extensive. The erasure of the requirement of authorization of standard contractual clauses in the rules regarding transfers by way of appropriate safeguards will be applauded by cloud computing businesses. The same goes for the codification of the rules regarding Binding Corporate Rules. Nevertheless, one should note that the current decisions and mechanisms, which will maintain their legal effect when the Regulation applies, are not always in line with the Regulation. This should be corrected within a reasonable period, but the drafting of the amendments or new decisions should definitely not be rushed. Another issue with the transfer to third countries is the disclosure of personal data to third countries (agencies, courts etc) which is not authorized by European legislation. This issue was solved in the interservice version of the proposed Regulation and the erasure of this solution should be reversed. The discussion on the rules regarding the transfers to third countries led to the following recommendations:

---

*The Commission should reform the procedure of adequacy decisions to enhance the effectiveness of article 41 of the proposed Regulation.*

*The decisions and mechanisms created under the regime of the current Data Protection Directive should be reviewed and amended/replaced in line with the Regulation, within a reasonable timeframe.*

*The Commission should introduce a new article with the content of article 42 of the interservice version of the proposed Regulation to prevent the unnecessary disclosure of personal data to entities from third countries.*

---

Finally, the proposed articles regulating the Supervisory Authorities are discussed in the third chapter of this thesis. The new rules are discussed in the light of cloud computing and with a positive result, primarily because it accents co-operation and consistency. The rules to have a one-stop-shop are welcomed as well. However there is a possibility of inequality between a multinational and the leading authority and a provision regulating the leading authority when a cloud provider does not have an establishment in a Member State is missing, which leads to the following advice:

---












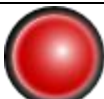

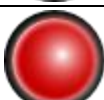

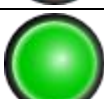
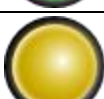


*The Commission should adopt rules to prevent the situation of an unequal conflict between a huge multinational and a relatively small supervisory authority, for instance by for instance by taking this into account while reviewing the budget provisions.*



*To fill the gap of the missing rules regarding the appointment of the leading authority when a cloud provider is not established in the Union, the Commission should adopt rules to solve this issue.*

---

One can conclude that the European legislator did a good job in improving the data protection rights of individuals while using cloud computing services and enhancing the free flow of data. However, the burden on cloud computing providers is increased tremendously and some of the rights and principles introduced in the proposed Regulation are disproportional or even unrealistic, this will have a chilling effect on the development and deployment of cloud computing in Europe. To become a 'world cloud computing powerhouse', the Commission has to solve these issues by taking the aforementioned recommendations into account. Then, the successor of the Data Protection Directive will be applauded by all the stakeholders of the cloud computing business.

VISUALIZATION

<b>Choice for a regulation</b>		§ 3.2	<b>Data Protection by default</b>		§ 3.11
<b>Material scope</b>		§ 3.3.1	<b>Representatives</b>		§ 3.12
<b>Territorial scope</b>		§ 3.3.2	<b>Documentation</b>		§ 3.13
<b>Data subject and personal data</b>		§ 3.5	<b>Data Breach Notification</b>		§ 3.14
<b>Controller and processor</b>		§ 3.4	<b>Data protection officer</b>		§ 3.15
<b>Consent</b>		§ 3.6	<b>Transfers with an adequacy decision</b>		§ 3.16.1
<b>Right to be forgotten</b>		§ 3.7	<b>Transfers by way of appropriate safeguards</b>		§ 3.16.2
<b>Right to data portability</b>		§ 3.8	<b>Existing decisions and mechanisms</b>		§ 3.16.3
<b>Right to object</b>		§ 3.9	<b>Disclosures not authorized by Union law</b>		§ 3.16.5
<b>Profiling</b>		§ 3.10	<b>Supervisory authority</b>		§ 3.17
<b>Data Protection by design</b>		§ 3.11			

	There are difficulties with the provision, but those can be solved by the recommendation(s) given.	
---	--	---

When the provision is suitable for cloud data rights of individuals while also promoting computing, contributes to the protection of the the free flow of data and the digital market, it will have the green light next to it. (minor difficulties are allowed).

# BIBLIOGRAPHY

## Legislation

### **Charter of Fundamental Rights of the European Union**

European Union, Charter of Fundamental Rights of the European Union, 7 December 2000, Official Journal of the European Communities, 18 December 2000 (2000/C 364/01).

### **Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data**

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28.I.1981, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm>> last visited 30 September 2012.

### **Data Protection Directive (DPD)**

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 – 0050.

### **Data Retention Directive**

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105 , 13/04/2006 p. 0054 – 0063.

### **E-Privacy Directive**

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), Official Journal L 201 , 31/07/2002 P. 0037 – 0047.

### **European Convention for the Protection of Human Rights and Fundamental Freedoms**

Council of Europe, European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS.

### **Regulation (EC) No 45/2001**

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, Official Journal L 008 , 12/01/2001 P. 0001 – 0022.

### **Treaty of Lisbon**

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007, 2007/C 306/01.

## Literature

### **Ambrust et al. 2009**

Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R.H., Konwinski, A., et al. (2009). Above the clouds: a Berkeley view of cloud computing'. *Technical report, EECS Department, University of California*, Retrieved January 30, 2013, from <http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.pdf>.

### **Ausloos 2012**

Ausloos, J. (2012). The 'Right to be Forgotten – Worth remembering?', *Computer Law & Security Review*, 28(2), 43-152.

### **Bainbridge 1997**

Bainbridge, D. (1997). Processing personal data and the data protection directive, *Information & Communications Technology Law*, 6(1), 17 - 40.

### **Balboni 2010**

Balboni, P. (2010). Data Protection and Data Security Issues Related to Cloud Computing in the EU. *Tilburg Law School Research Paper No. 022/2010*.

### **Barros & Dumas 2006**

Barros, A., & Dumas, M. (2006). The Rise of Web Service Ecosystems. *IT Professional*, 8(5), 31-37.

### **Blume 2012**

Blume, P. (2012). Will it be a better world? The proposed EU Data Protection Regulation. *International Data Privacy Law*, 2(3), 130-136.

### **Bygrave 2000**

Bygrave, L. (2000). European Data Protection - Determining applicable law pursuant to European Data Protection Legislation. *Computer Law and Security Report*, 16(4), 252-257.

### **Bygrave 2001**

Bygrave, L. (2001). The Place of Privacy in Data Protection Law. *University of New South Wales Law Journal*, 24(1), 277 - 283.

### **Bueno 2010**

Buono, L. (2010). The global challenge of cloud computing and EU law. *Eurcrim*, 3 (1), 171 - 122.

### **CDT Analysis 2012**

Center for Democracy & Technology. (2012). CDT Analysis of the proposed data protection regulation. Retrieved January 30, 2013, from <https://www.cdt.org/files/pdfs/CDT-DPR-analysis.pdf>.

### **Chester 2012**

Jeff, C. (2012). Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the "Big Data" Era. *European Data Protection: In Good Health?* (pp. 53-77). Dordrecht: Springer Netherlands.

**Craig & de Búrca 2011**

Craig, P. P., & Búrca, G. (2011). *EU law: text, cases, and materials*. Oxford: Oxford University Press.

**Geelan 2009**

Geelan, J. (2009). Twenty-one experts define cloud computing. *Cloud computing journal*, Retrieved January 30, 2013, from <http://cloudcomputing.sys-con.com/node/612375>.

**Gens 2012**

Gens, F. (2012). *IDC predictions 2012: Competing for 2020. Report*.

**Goldsmith & Wu 2008**

Goldsmith, J. L., & Wu, T. (2008). *Who controls the Internet?: illusions of a borderless world*. New York: Oxford University Press. (Original work published 2006).

**Grobauer et al. 2011**

Grobauer, B., Walloschek, T., & Stocker, E. (2011). Understanding Cloud Computing Vulnerabilities. *Security & Privacy, IEEE*, 9(2), 50-57.

**De Hert P. & Gutwirth 2009**

Hert, P. D., & Gutwirth, s. (2009). Data protection in the case law of Strasbourg and Luxemburg: constitutionalisation in action. *Reinventing Data Protection?* (pp. 3 - 44). Dordrecht: Springer Netherlands.

**De Hert & Papakonstantinou, 2011**

Hert, P. D., & Papakonstantinou, V. (2011). The Amended EU Law on ePrivacy and Electronic Communications. *The John Marshall Journal of Computer & Information Law*, 29(1), 29 – 74.

**De Hert & Papakonstantinou, 2012**

Hert, P. D., & Papakonstantinou, V. (2012). The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals. *Computer Law & Security Review*, 28(2), 130-142.

**Hon et al. 2011 A**

Hon, W. K. et al. (2011). The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing. *International Data Privacy Law*, 2011, 1(4), 211 – 228.

**Hon et al. 2011 B**

Hon, W. K. et al. (2011). Who is Responsible for 'Personal Data' in Cloud Computing?. *International Data Privacy Law*, 2(1), 3-18.

**Hon et al. 2011 C**

Hon, W. K. et al. (2011). Data Protection Jurisdiction and Cloud Computing – When are Cloud Users and Providers Subject to EU Data Protection Law? *Queen Mary School of Law Legal Studies Research Paper No. 84/2011*.

**IDC 2012**

International Data Corporation. (2012). *Quantitative Estimates of the Demand for Cloud Computing in Europe and the Likely Barriers to Take-up. Final Report*.



**Korff 2008**

Korff, D. (2008). Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons. Retrieved January 30, 2013, from <http://ssrn.com/abstract=1288583>.

**Korff 2012**

Korff, D. (2012). Comments on selected topics in the draft EU Data Protection Regulation Retrieved January 30, 2013, from <http://ssrn.com/abstract=2150145>.

**Kuner 2010**

Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 2). *International Journal of Law and Information Technology*, 18(3), 227 – 247.

**Kuner 2012**

Kuner, C. (2012). The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. Prepared for *the Privacy and Security Law Report by The Bureau of National Affairs*, 1-15.

**Leenes 2010**

Leenes, R. (2010). Who Controls the Cloud? *IDP: Internet, law and politics e-journal*, 2010(11), 1-10.

**Mahowald et al.2011**

Mahowald, R.P., Konary, A. & Sullivan, C.G. (2011). Market Analysis Perspective: Worldwide Saas & Cloud Services, 2011: New Models for Delivering Software. *IDC Report*.

**Moerel 2011 A**

Moerel, E. M. L. (2011). Back to basics: when does EU data protection apply? *International Data Privacy Law*, 1(2), 92-110.

**Moerel 2011 B**

Moerel, E. (2011). *Binding corporate rules: Fixing the regulatory patchwork of data protection*. Amsterdam.

**Pattison 2012**

Pattison, M. (2012). Updated guidance on data breach notification. *Keeping Good Companies*, 64(7), 388-390.

**Poullet et al. 2010**

Poullet, Y., Gyseghem, J., Gérard, J., Gayrel, C., & Moiny, J. (2010). Cloud computing and its implications on data protection. *Council of Europe Discussion Paper (DRAFT)*. Retrieved January 30, 2013, from [http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079\\_reps\\_IF10\\_yvespoullet1b.pdf](http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Reports-Presentations/2079_reps_IF10_yvespoullet1b.pdf).

**Reding 2012**

Reding, V. (2012). The European data protection framework for the twenty-first century. *International Data Privacy Law*, 2(3), 119 – 129.

**Robinson et al. 2011**

Robinson, N., Valeri, L., Cave, J., Thompson-Starkey, T.G., Graux, H., Creese, S. & Hopkins, P. (2011). The Cloud Understanding the Security, Privacy and Trust Challenges, *Technical report of RAND Europe, TR-933-EC*. Retrieved January 30, 2013, from [http://www.rand.org/pubs/technical\\_reports/TR933.html](http://www.rand.org/pubs/technical_reports/TR933.html).

**Rosen 2012**

Rosen, J. (2012). The Right to Be Forgotten. *Stanford Law Review Online*, 64, 88 – 92. Retrieved January 30, 2013, from <http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf>.

**Sartor 2013**

Sartor, G. (2013). Providers' liabilities in the new EU Data Protection Regulation: A threat to Internet freedoms? *International Data Privacy Law*, 3(1), 3 – 12.

**Schreurs et al. 2008**

Schreurs, W., Hildebrandt, M., Kindt, E. & Vanfleteren, M. (2008). Cogitas, Ergo Sum. The Role of Data Protection Law and Non-discrimination Law in Group Profiling in the Private Sector. Profiling the European citizen cross-disciplinary perspectives (pp. 241 - 270). New York: Springer.

**Swire & Lagos 2012**

Swire, P. & Lagos, Y. (2012). Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique. *Maryland Law Review, Forthcoming; Ohio State Public Law Working Paper Forthcoming*.

**Vaquero et al. 2008**

Vaquero, L., Merino, L., Caceres, J., & Lindner, M. (2008). A break in the clouds: towards a cloud definition. *SIGCOMM Comput. Commun. Rev.*, 39(1), 50-55.

**Wong, R & Savirimuthu (2008)**

Wong, R. & Savirimuthu, J. (2008). All or nothing, this is the question: The application of Article 3(2) Data Protection Directive 95/46/EC to the Internet. *John Marshall Journal of Computer & Information Law*, 25(2), 241 – 266.

**Official documents****CoE Recommendation 2010**

Council of Europe, *Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling*, 23 November 2010.

**Cloud Computing Hearing with Telecommunication and Web Hosting Industry 2011**

Cloud Computing Hearing with Telecommunication and Web Hosting Industry, Meeting Note, 16 November 2011. Available at [http://ec.europa.eu/information\\_society/activities/cloudcomputing/docs/hearingreport-telecomsv2.pdf](http://ec.europa.eu/information_society/activities/cloudcomputing/docs/hearingreport-telecomsv2.pdf) > last visited 23 January 2013.

### **EC Expert Group Report 2010**

Commission of the European Communities, Information Society and Media, Expert Group report, *The Future of Cloud Computing – Opportunities for European Cloud Computing Beyond 2010*, 2010.

### **EC communication 2010**

Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A comprehensive approach on personal data protection in the European Union*, COM (2010) 609 final, 4 November 2010.

### **EC communication 2012 A**

Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Safeguarding Privacy in a Connected World A European Data Protection Framework for the 21st Century*, COM (2012) 9 final, 25 January 2012.

### **EC communication 2012 B**

Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - Unleashing the Potential of Cloud Computing in Europe*, COM(2012) 529 final, 27 September 2012.

### **EC Impact Assessment 2012**

Commission of the European Communities, Commission Staff Working Paper, *Impact Assessment*, SEC(2012) 72 final, 25 January 2012.

### **EC Executive Summary of the Impact Assessment 2012**

Commission of the European Communities, Commission Staff Working Paper, *Executive Summary of the Impact Assessment*, SEC(2012) 73 final, 25 January 2012.

### **EC report 2003**

Commission of the European Communities, *First Report on the implementation of the Data Protection Directive (95/46/EC)*, COM (2003) 265, Brussels, 15 May 2003.

### **EDPS opinion 2012**

European Data Protection Supervisor, *Opinion of the European Data Protection Supervisor on the data protection reform package*, 7 March 2012.

### **ENISA 2009**

The European Network and Information Security Agency (ENISA), *Cloud computing, Benefits, risks and recommendations for information security*, 2009 .

### **General Data Protection Regulation Proposal 2012 (or: the proposed Regulation)**

Commission of the European Communities, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM (2012) 11 final, 25 January 2012.

### **Draft of General Data Protection Regulation Proposal 2012 (or: Interservice version of the proposed Regulation)**

Commission of the European Communities, *Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, Draft Version 56, 29 November 2011, available at <<http://www.statewatch.org/news/2011/dec/eu-com-draft-dp-reg-inter-service-consultation.pdf>> last visited 30 January 2013.

### **LIBE Draft Report 2013**

Jan Philipp Albrecht, Committee on Civil Liberties, Justice and Home Affairs, *DRAFT REPORT on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM(2012)0011 – C7-0025/2012 – 2012/0011(COD).

### **Mell & Grance 2011**

P. Mell and T. Grance, National Institute of Standards and Technology, *The NIST Definition of Cloud Computing* (Special Publication, 800-145, 2011).

### **Liu et al. 2011**

Liu et al., National Institute of Standards and Technology, *NIST Cloud Computing Reference Architecture* (Special Publication 500-292).

### **WP 12**

Article 29 Working Party, *Working document on transfers of personal data to third countries : Applying Articles 25 and 26 of the EU data protection directive*, DG XV D/5025/98 WP 12, adopted on 24 July 2008.

### **WP56**

Article 29 Working Party, *Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites*, 5035/01/EN/Final WP 56, adopted 30 may 2002.

### **WP 136**

Article 29 Working Party, *Opinion 4/2007 on the concept of personal data*, 01248/07/EN WP 136, Adopted on 20 June 2007.

### **WP 153**

Article 29 Working Party, *Opinion Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules*, 1271-00-00/08/EN WP 153, Adopted on 24 June 2008.

**WP 163**

Article 29 Working Party, *Opinion 5/2009 on online social networking*, 01189/09/EN WP 163, Adopted on 12 June 2009.

**WP 168**

Article 29 Working Party, *The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, 02356/09/EN WP 168, Adopted on 01 December 2009.

**WP 169**

Article 29 Working Party, *Opinion 1/2010 on the concepts of "controller" and "processor"*, 00264/10/EN WP 169, Adopted on 16 February 2010.

**WP 173**

Article 29 Working Party, *Opinion 3/2010 on the principle of accountability*, 00062/10/EN WP 173, adopted 13 July 2010.

**WP 179**

Article 29 Working Party, *Opinion 8/2010 on applicable law*, 0836-02/10/EN WP 179, adopted 16 December 2010.

**WP 191**

Article 29 Working Party, *Opinion 01/2012 on the data protection reform proposals*, 00530/12/EN, WP 191, adopted on 23 March 2012.

**WP 196**

Article 29 Working Party, *Opinion 05/2012 on Cloud Computing*, 01037/12/EN, WP 196, adopted 1 July 2012.

**WP 199**

Article 29 working party, *Opinion 08/2012 providing further input on the data protection reform discussions*, 01574/12/EN, WP 199, Adopted on 05 October 2012.

**Cases**

CJEU case 230/78, *SpA Eridania-Zuccherifici nazionali and SpA Società Italiana per l'industria degli Zuccheri v Minister of Agriculture and Forestry, Minister for Industry, Trade and Craft Trades, and SpA Zuccherifici*, [1979] ECR02749.

CJEU case 168/84, *Gunter Berkholz v Finanzamt Hamburg-Mitte-Altstadt*, ECR [1985] p. 2251. (Bergholz).

CJEU case C-390/96, *Lease Plan Luxembourg SA v Belgian State*, ECR [1998] p. I-2553 (Lease Plan).

CJEU case C-221/89, *The Queen v Secretary of State for Transport, ex parte Factortame Ltd and others*, [1991] ECR I-3905. (Factortame).

CJEU case C-101/2001, *Bodil Lindqvist*, 6 November 2003. (Lindqvist).

CJEU case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, [2008] ECR I-09831. (Satamedia).

CJEU Case C-518/07, *European Commission v Federal Republic of Germany*, [2010] ECR I-01885.

## Websites

<<http://bits.blogs.nytimes.com/2012/07/24/twitter-is-working-on-a-way-to-retrieve-your-old-tweets/>> last visited 30 January 2013.

<<https://www.dropbox.com/help/7/en>> last visited 30 January 2013.

<[http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/passenger-name-record/index\\_en.htm](http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/police-cooperation/passenger-name-record/index_en.htm)> last visited 30 January 2013.

<[http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index\\_en.htm](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/index_en.htm)> last visited 30 January 2013.

<[http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/transfer/index_en.htm)> last visited 30 January 2013.

<[http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm)> last visited 30 January 2013.

<[http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index\\_en.htm](http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm)> last visited 30 January 2013.

<[http://ec.europa.eu/justice/news/consulting\\_public/news\\_consulting\\_0003\\_en.htm](http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm)> last visited 30 January 2013.

<[http://ec.europa.eu/justice/news/consulting\\_public/news\\_consulting\\_0006\\_en.htm](http://ec.europa.eu/justice/news/consulting_public/news_consulting_0006_en.htm)> last visited 30 January 2013.

<[http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13\\_Speech\\_Cloud\\_Computing\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2010/10-04-13_Speech_Cloud_Computing_EN.pdf)> last visited 30 January 2013.

<[http://export.gov/safeharbor/eu/eg\\_main\\_018475.asp](http://export.gov/safeharbor/eu/eg_main_018475.asp)> last visited 30 January 2013

<<https://www.facebook.com/help/131112897028467/>> last visited 30 January 2013.

<<https://www.facebook.com/help/210644045634222/>> last visited 30 January 2013.

<<http://www.google.com/about/company/facts/locations/>> last visited 30 January 2013.

<<https://www.google.com/takeout/>> last visited 30 January 2013.

<<http://investor.google.com/financial/2011/tables.html>> last visited 30 January 2013.

<<http://leidenlawblog.nl/articles/the-dutch-cookie-conundrum>> last visited 30 January 2013.

<<http://www.ncsl.org/issues-research/telecom/overview-security-breaches.aspx>> last visited 30 January 2013.

<[http://news.cnet.com/8301-13953\\_3-10052188-80.html](http://news.cnet.com/8301-13953_3-10052188-80.html)> last visited 30 January 2013.

<<http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm>> last visited 30 January 2013.

<<http://peterfleischer.blogspot.nl/2011/03/foggy-thinking-about-right-to-oblivion.html>> last visited 30 January 2013.

<<http://support.google.com/mail/bin/answer.py?hl=en&answer=6603>> last visited 30 January 2013.

<<http://support.google.com/accounts/bin/answer.py?hl=en&answer=1350409>> last visited 30 January 2013.

<<http://thepiratebay.se/blog/210>> last visited 30 January 2013.

<<http://www.zdnet.com/blog/btl/google-wins-floating-data-center-patent/17266>> last visited 30 January 2013.

<<http://www.zdnet.com/news/hp-dismisses-cloud-hype/255222>> last visited 30 January 2013.