Extended Abstract: The new paradigm of Data Protection and the Impact on Cloud Computing

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

I. INTRODUCTION

The recent digital era has given rise to an exceptionally high degree of personal data and information sharing. This has led to many countries being faced with the debate, and concern, of going about protecting rights, especially those concerning personal individual rights. Recently, the European Union has also dedicated itself to enhance the Data Protection rights with the implementation of the General Data Protection Regulation (GDPR).

With the rise of cloud computing, the problem concerning geographical location of the several infrastructures which house data has emerged, especially in regards to the fact that data is stored across countries within the E.U and 3rd part countries. The European Commission now has to deal with how to analyze and protect personal information within the realm of the GDPR.

While the transmission of data across frontiers is one of the main preoccupations relating to cloud computing, it is important to highlight the role that Cloud Service Providers play, these entities assumed less responsibilities due to Directive 95/46/CE, however, with the GDPR, they are now seeing their respective responsibilities shifting.

This extended abstract aims to summarize the thesis and to showcase several problems that have arisen in regards to the protection of data when it crosses frontiers to 3rd party countries as well as to analyze the responsibility which Cloud Service Providers have in protecting these personal rights be it as the main responsible party, the controller, or as sub-contractors, a processor [1].

II. HISTORICAL RELEVANCE

The concept of information security data protection, as we know them today, differs greatly from what they were for our ancestors. We can consider that the concern of protecting information goes back to the oldest exchanges of letters, and other documents, that would leave one party, guarded, and arrive at the intended destination untouched.

One of the first ways to ensure the protection of information was encryption. Dating back to the 5th century BC, the Greeks came up with the first known military encryption system. Cryptanalysis came to fruition in the first century AD. There are documents detailing the various types of cryptography from this time period which included transposition and substitution systems.

In Europe, cryptology began to develop in Italy during the early fifteenth century. The emergence of diplomacy led to a great evolution in cryptology due to embassies regularly sending letters to one another using encryption to make them indecipherable. [2]

This evolution grew even more pronounced during war time as the increasing concern of the states regarding the privacy of their information became a priority. In 1940, during World War II, the enigma machine was used by the Germans to encrypt their communications. To counteract this, Alan Turing was responsible for the emergence of the first computer with the aim of deciphering German messages.

During the early 1970's there was an increase in the use of computers and, at the same time, the Advance Research Projects Agency (ARPA) of the United States Department of Defense developed a small network comprised of four computers, giving emergence to the very beginning of what we know today as the internet.

Although information security and data protection are much more comprehensive than cyber security, the interconnection of technological developments with the growing concern for data protection is undeniable.

The current technological evolution and an increase in international trade have opened new doors for the processing of data at an international scale. And although these developments have offered great advantages as far as efficiency and productivity are concerned, they have also brought with it awareness regarding the importance for the privacy of individuals.

III. LEGAL FRAMEWORK& CLOUD COMPUTING

From a legal point of view, the first that should be considered is the Universal Declaration of Human Rights [2] which concerns the basis for the protection of individual rights.

The Declaration of Human Rights was adopted by the United Nations General Assembly on December 10, 1948, in Paris, France. This declaration contains specific provisions concerning the right to private and

Extended Abstract: The new paradigm of Data Protection and the Impact on Cloud Computing

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

family life. The principles outlined in the Declaration of Human Rights have in fact provided the basis for most of the data protection laws which have since come into play.

From the late 1960s through the 1980s, a number of countries, especially European countries, debated on the control and use of personal information both by private entities as well as the government itself. In three European countries, Spain [3], Portugal, and Austria [4], data protection has also been incorporated as a fundamental right within their respective Constitutions.

In 1973 and 1974, the European Council relied on resolutions 73/22 [5] and 74/29 [6] with the aim of establishing principles for the protection of personal data found in automated databases in the public and private sectors. The aim would be to promote a standard for the homogeneity for the national laws of the Member States. It has now become imperative to create binding international standards so as to not allow divergence of domestic legislation. In 1980, and with basis on the aforementioned, that the European Council issued the first binding international instrument laying down standards for the protection of the personal data of persons: the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [7]. In that Convention also called Convention 108, the European Council ruled that persons dealing with personal information on a digital medium have a responsibility to protect such data.

In 2001, the Additional Protocol to the Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data was opened for signature and concerned the control authorities and cross-border data flows. This protocol came in force in July 2004 being applied in Portugal in 2007. The objective of the design of this additional Protocol was to establish an approach to measures concerning the transfer of personal information to countries that were not signatories to Convention 108. The solution to this is found in Article II of the Protocol, with the cross-border flow of personal data to an addressee who is not subject to the jurisdiction of a Party to the Convention.

In the decades following the appearance of the first computers and the first networks, computing was almost entirely centralized. It was during 100th anniversary commemorative speech of MIT that the term *Cloud Computing* first appeared. John McCarty was the first to speak publically of the idea, proposing a method referred to as Time Sharing, which entailed sharing the processing power of various machines and thusly leveraging their capabilities. This idea, although popular at the time, was quickly been forgotten at the time as the hardware, nor the software, were prepared for this new era. With the emergence, in the 1980s, of better and cheaper microprocessors, personal computers, and Unix-based workstations, was this idea revisited, and with it paved the way for the new distributed client-server-based computing model.

With the advent of the Internet and its subsequent privatization in 1991, the Internet ceased to be in the public domain and moved into the realm of the private domain, with the first private Internet distributors started to appear, thusly increasing its growth and diffusion. In the same decade, Robert Cailliau, published a proposal for what would become known as the World Wide Web. This network was designed in order to make available hypermedia documents, these being connected to one another and being executed through the internet [8].

In 1993, CERN announced that the World Wide Web, also known as WWW, would be free for all at no cost. The WWW, although not the only service available through the internet, had quickly become the most popular, largely due to the protocols used, namely the hypertext transfer protocol known as HTTP, a protocol of the application layer Open System Interconnection model used for data transfer within the WWW. In practice, the HTTP protocol communicates between the client and server through messages. The client sends a message with the purpose of requesting a resource and the server then sends a response message to the client with the request. While most web-based applications used to follow the client-server model at this time, as the Internet and the World Wide Web became more and more popular globally, the need for a new computing model became increasingly clear, a model that would go beyond centralized and client-server models, the model that today become known as the Cloud.

The growing number of users accessing web applications was increasing the demand for servers that were increasingly scalable. Due to this, the emergence of data centers came to fruition. Several

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

factors, such as the ability to share work and the provision of sophisticated systems management tools, led to a large scale migration of services to this model.

After these events, the Cloud model once again came into play. With the passage of time and exponential innovation, the first of the "Software as a Service" models began to emerge. One of these early projects was SalesForce.com, which has developed a business model based on on-demand services. Since 2000, and with awareness of the importance of this phenomenon, Microsoft and IBM started working on their own Cloud services. In 2005, Amazon launched the Amazon Web Service, where it adapted its data centers to this new reality. In the years that followed both Google and Microsoft developed their own tools.

IV. TECHNOLOGICAL BACKGROUND OF CLOUD COMPUTING

In its simplest form, cloud computing offers a simple way to access servers, storage, information banks and other services over the Internet.

The cloud consists of three components: storage, nodes and a controller. According to NIST, the cloud is "a model that conveniently deploys the on-demand network intro a shared set of configurable computing resources (e.g. networks, servers, storage, applications and services) that can be quickly delivered effortlessly with minimum management or intervention by the service providers"[8]. However, the truth is that defining cloud computing has always generated controversy in the community; the problem is that so many companies use the cloud with objectives and in different ways. Thus, it is seen that any form of network-accessible computing and almost any type of activity that involves access to mass datasets is within the scope of cloud computing [9].

For some, the cloud is about web searches, for others it is about social networking, while others still think of the cloud as a form of outsourcing technology, allowing one to send data to a remote location where computing and storage are cheaper. All of these ways of perceiving the cloud are considered to be absolutely correct.

Along with the individual perceptions of what cloud computing is, the respective definition also varies greatly. IBM described cloud computing or, the cloud, as the delivery of on-demand computing resources – from applications to data centers – to the internet on a per-use basis. Amazon describes the model as "delivering on-demand computing power, database storage, applications and other IT resources through a cost-per-use Internet-based cloud services platform". [10]

There are three main service models for cloud computing: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

Through the IaaS system, the user has at their disposal all computational infrastructure resources, without having to worry about the hardware of the continuity of the service in the event of a failure due to it being up to the service provider to deal with these lower-level aspects. For example, the resources can be network resources, servers, and storage space, among others.[11]

In regards to the PaaS system, there is no underlying question regarding the infrastructure on which the platform is based, as this concern will be the responsibility of those who offer the IaaS service. In practice a platform is provided so that the entity can develop and manage its software. In this case, there are less burdens, but there is also less flexibility. The act that this system is less portable is a major disadvantage, an example of this being in the case of SalesForce, due to its database and programming language being "closed code", an application can only be developed using the programming language Apex, and can only be executed within the cloud infrastructure from SalesForce.com [11].

The SaaS system is often used to identify a software application that works in the cloud. It is a software distribution model that allows or the use of application exclusively through a browser. Due to this the user has knowledge of where the software is hosted, in which operating system it is executed and in which programming language it was developed. Locally there is no need for installation and only one browser is required. Examples of SaaS include email services Client Relationship Management (CRM), or storage services such as OneDrive, Dropbox, and GoogleDrive. This type of service is usually billed periodically based on the number of active users [12].

Extended Abstract: The new paradigm of Data Protection and the Impact on Cloud Computing

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

There are four main types of cloud development models: private cloud, public cloud, community cloud and hybrid cloud.

The private cloud, also referred to as the internal cloud, is an infrastructure developed and managed exclusively for an entity, or group of entities. This type of cloud may be owned or run on a leasing model. Depending on the location or leasing, the location may be internally housed or hosted abroad on a third-party infrastructure. This model provides the cloud owner greater security and control of infrastructure resources and customers. NIST describes the private cloud as "an infrastructure within the client's property". In terms of costs, and since the organization acquires and manages the entire infrastructure, this model will be more expensive than other models, such as the public cloud model. Examples of a private cloud include VMware and SalesForce [1].

The public cloud, also referred to as the external cloud, is a resource made available by a cloud provider. In this model, the ownership of the cloud infrastructure comes from an organization that sells to the general public or to a company. This is the most utilized model, being available simply by accessing the internet. Unlike the private cloud, the risk management of the infrastructure will not be for the entity that is using the cloud for rather for the Cloud Provider. However, data security and privacy are also lesser, due to the fact that it is the provider who manages the infrastructure; this deprives the customer of the control and management of the physical and logical security of the infrastructure.[12] NIST describes this cloud model as an "infrastructure located within the supplier's property that is provisioned for use open to the general public, and ownership, management and operation may be carried out by business, academic or governmental organizations". Examples of a public cloud model include Amazon Elastic Compute Cloud, IBM BlueCloud, SunCloud, Google AppEngine and Windows Azurre Services Platform. The costs of this type of cloud model are lower compared to the private cloud [1].

The community cloud, as the name implies, entails a sharing of infrastructure and resources, it can be said that this model can be placed between the private and public cloud. The community cloud, defined by NIST is "an infrastructure shared by multiple organizations, belonging to a specific community and sharing common goals such as the mission, security requirements, as well as compliance policies and considerations. The management can be carried out by the organizations or by third parties and their location is internal or external" [1].

The hybrid cloud is formed by combining other models such as public, private or community. NIST defines the hybrid cloud model as "a combination of two or three models (public, private and community) which continue to exist in isolation, but are integrated through proprietary or open technology which enable portability and mobility of information and applications.".[1] The purpose of this model is to reduce the disadvantages of the models described above by having a more flexible product that allows the private cloud to be used for more sensitive information or data and to a public cloud for less sensitive data [12].

V. DATA PROTECTION: THE GENERAL REGULATION ON DATA PROTECTION

Although other countries have their own internal laws, for the purposes of this thesis the focus is on the active General Data Protection Regulation (GDRP) laws within the European Union. The GDRP and the European Data Protection Regulation (EU) 2016/679 of the European Parliament and will be referred to solely considered to be European data protection legislation. The GDPR dates from April 27, 2016 and has been applied directly from May 25, 2018.[13]

The GDPR applies to the 28 Member States because it does not need to be transposed into national law and due to that fact it has harmonized data protection within the European Union.

The GDPR repeals Directive 95/46/EC providing new rights for data owners such as the right to portability of data, the right to forgetfulness and the right to object, which will be discussed in detail within the thesis itself. It also brings some alterations to data controllers and processors, which is particularly relevant to the cloud.

Regarding the definition of personal data, the General Regulation in Article 4, defines personal data as "information relating to an identified and identifiable natural person (data subject); an identifiable person shall be considered to be identifiable, directly or indirectly, in particular by reference to an identifier, such as name, an identification number, location data, electronic identifiers of one or more specific elements

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

of the identifier, physical physiological, genetic, mental, economic, cultural or social identity of the natural person" [13].

At the national level, the Constitution of the Portuguese Republic also provides for the right to privacy and protection of personal data of each individual in Articles 26 and 35. Article 26 provides that "everyone shall have the right to personal identity, personality development, civil capacity, citizenship, good name and reputation, image, speech, privacy and privacy to legal protection against any form of discrimination" [14]. Article 35 of the Portuguese Constitution concerns the use of information technology.

Regarding the concept of processing, the definition of Article 4, defines processing thereof as "an operation or set of operations carried out on personal data or on a set of personal data by automated or non-automated means such as collection, organization, structuring, preservation, adaptation, or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other form of making available comparison or interconnection, limitation erasure, or destruction".[13]

In regards to consent, and Article 14 of the General Data Protection Regulation, this is defined as "a free, specific, informed and explicit manifestation of well, by which the holder by means of a statement or an unequivocal positive act, that personal data relating to this is processed".[13]

Regarding the rights of data owners, the new regulation as introduced or reformulated several rights. This thesis will define the rights of data owners as the right to be informed of the location of the data in order to exercise the rights as access, rectification, erasure, portability and / or opposition.

The right to transparency is above all, the right to be informed of the rules for the exercise of all other rights at their disposal. This information should be transmitted using clear and simple language, with special emphasis on communication with children.[13]

The right to information is based on information that must be provided to the holder of the data, as far as the GDPR is concerned this right is outlined in Articles 13 and 14 where the information to be provided to the holder is nominated. Information provided will depend on whether the data is collected with or without the holder. Article 13 of the GDPR states, "information is to be provided when personal data is collected from the holder".

The right of access to the data subject is based on the right that the data subject must obtain the information, knowing whether or not his or her data is being processed and has the ability to access that data. Article 15, Paragraph 3, states that for this right to be fulfilled, the controller must provide the holder with "a copy of the personal data in the process of being processed", which may be physical or electronic as well as the payment of a fee for administrative costs.

The right to rectification concerns the right of the data subject to rectify his data, such as data that is outdated, incomplete or even inaccurate. Article 16 of the GDPR states that "the holder has the right to obtain … from the controller the correction of inaccurate personal data concerning him. In view of the purposes of processing, the data subject has the right to incomplete personal data, including by means of an additional declaration."[13]

The right to be forgotten, or the right to oblivion, has origin in a French law coming from the expression "le droit à l'oubli". The French legal system deals with this right by which an individual who has served a criminal sentence may object to the publication of the facts of his conviction after having served the sentence. In 2012, the Vice President for the European Commission, Viviane Reding, proposed to the European Parliament to regulate the right to forget because "it is important to give people control over their data: the right to be forgotten … people will have the right – and not just the "possibility" – to withdraw their consent for the processing of the personal data they have given themselves.[15] The Internet has a capacity for searching and memory that is nearly unlimited. Even tiny remnants of personal information can have a huge impact … the right to be forgotten will build on existing rules to better handle privacy risks online. It is the individual who should be in the best position to protect the privacy of their data, choosing whether or not to provide them". Thusly, in 2012, the European Commission initiates work on legislative review, including in this revision a Regulation for the Protection o Personal Data, where the right to be forgotten was first introduced.

Extended Abstract: The new paradigm of Data Protection and the Impact on Cloud Computing

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

The obligation to notify the rectification or erasure of personal data or limitation of treatment has also become a right. According to this Article, the data controller must inform the data subject when their personal data has been rectified or erased or if there has been a limitation to the treatment in accordance with Article 16 and 18 of the regulation. This notification does not have to be made only if the communication proves impossible or involves a disproportionate effort. The controller must also provide the holder with information on the recipients if so requested by the data subject.[13]

The right to portability is a new one and is stated in the GDPR. This right, although having only come into effect with the GDPR, had already been mentioned in the Resolution of the European Parliament of 2011. The scope of this right pertains to the data subject being able to transfer their data easily and quickly from one service provider to another. This right seeks to simplify the data subject being able to transmit their personal data. The data controller, to whom portability has been requested, is obliged to make the data available to the subject in a format that can be easily transferred to the new provider.[13]

The right to opposition is the right which enables the data subject to have the right at any time to object to the processing of their respective data. Although the right o objection is not a new one, the GDPR has introduced new development with regards to automated data processing. Article 21 states that "the data subject has the right to object at any time … to the processing of personal data concerning him … including the definition of profiles on the basis of these provisions. The controller shall cease the processing of personal data unless he submits overriding and legitimate reasons for such processing which prevail over the interests, rights and freedoms of the data subject, or for the purposes of declaration, exercise or defense of a right in a data judicial process." [13]

VI. OBLIGATIONS OF THE ENTITIES: GDPR VS CLOUD ACTORS?

First of all we shall define what is a controller, a processor and a 3rd party.

A controller as said based on article 4 of GDPR "means the natural or legal person, public authority, agency or 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 such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law". A processor based on the same article, "means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". As a 3rd party "means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorized to process personal data".[13]

The obligations of the subcontractor towards the controller must be specified in a contract or other legal act. For example, the contract must indicate what happens to personal data once it is completed In regards to subcontracting by the subcontractor, the subcontractor can only do so with a prior authorization of the data controller. The role of the subcontractor is particularly important in the context of cloud.

The role of the CSP will be further investigated and discussed, which can take the form of data controller or sub-processor. In terms of the Cloud Service Provider (CSP), this is considered to be the entity that makes cloud services accessible. Just as there are electric and water suppliers, the CSP also functions as and takes the role of service provider.

When data is placed in the cloud, there is a perception of making this data public or that there is a loss of control over the data, and whether or not personal data remains protected. As mentioned in Article 4 of the GDPR, personal data is any data that makes a person identifiable and, even in the cloud; this data continues to be under the protection and protection of regulation as well as any other means of protection.

The problem lies not in the definition of the CSP, but in its role. There is difficulty in understanding whether the CSP is considered to be the data controller or a subcontractor.
The answer to this question is that it simply depends on each particular situation, i.e. the CSP will act as a subcontractor when it is contracted by a controller and does not process the data for its own benefit, this will be the most common case. However, when the CSP

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

treats the information for its direct benefit, it will become responsible for the processing. [16]

Considering the CSP as a controller, Directive 95/46/EC has imposed several obligation on what are considered to be controllers. In the event that the CSP acts as a processor through a contract with the party responsible for processing, the CSP is to be held liable for breach of contract only. Unlike the Directive, the GDPR is very clear about the added responsibilities of the processor, and makes reference to this in Article 5, "the controller shall be responsible for compliance with paragraph 1 and must be able to prove it".[13]

Considering the CSP as a processor, the GDPR has introduced many new responsibilities to processors than the Directive, making these added responsibilities apply directly to them. Due to this, processors, as well as controllers should keep written records on all categories of processing of personal data and activities carried out on behalf of the controller. It is imperative to both the controller, and where applicable, the processor, to make these records available to the supervisory authority upon request.

VII. DATA SECURITY – IMPACT ASSESSMENTS DATA BREACH NOTIFICATIONS

The GDPR has made clear and significant changes in data security. It requires, for example, that controllers apply appropriate measures to ensure and prove compliance with the GDPR.

In regards to a personal data breach, the GDPR requires that the data controller notify the authorities to monitor any breach of personal data, whenever possible, within 72 hours of becoming aware of such a breach. Such notification will not take place only if the breach does not result in a risk to the rights and freedoms of the data subjects. The controller is also required to provide notification of the reasons for delay if it fails to notify authorities within 72 hours. The notification will describe the nature of the breach of personal data as well as communicate the name and contact details of the data protection officer and will also describe the likely consequences of the breach of personal data and the measures taken or proposed by the controller to repair the violation of personal data. The data breach notification obligations do not only apply to the data controller, but also to the processor, stating that, under Article 2, they also have the obligation to notify the data controller after becoming aware of a violation of personal data [13].

The impact assessment of a data breach now must adhere to Article 35 of the GDPR. The party responsible, "when a certain type of treatment, in particular using new technologies and having regard to their nature, scope and context and purpose, is likely to entail a high risk to the rights and freedoms of natural persons" are obliged to initiate data processing to make an assessment o the impact of operations on personal data. After the impact assessment has been carried out, the controller, if necessary, may carry out a verification to confirm if the treatment is being carried out in accordance with the impact assessment.[13]

VIII. DATA TRANSFER TO 3RD PARTY COUNTRIES – A GLOBAL PERSPECTIVE

Due to the new global era, the collection and sharing of personal data has increased almost exponentially. New technologies have given public and private entities increasing access to personal data. The burden is not only on these entities but also on the data subjects, who, largely due to social networks, disseminate their data on a scale that has never before been seen. These advances have led to an enormous increase in the circulation of personal data both within the European Union and to 3rd party Countries. In this sense, it is vital that this data be protected. Article 44, which establishes the general principle of transfers, transfers of data which are processed after being transferred to a third country or international organization are only respected by the data controller and processors of the conditions set forth by the GDPR.

When data transfers occur within the European Union, the level of protection provided by the GDPR must be guaranteed. The more pressing concern is the protection of data transferred to a third country or international organizations. What is emphasized, and from what is stated in Memorandum 101, is that "transfers to 3rd party countries and international organizations can only be carried out in full respect to this Regulation. Data transfers may only be made if the other provisions of this Regulation are complied with for the transfer of personal data to third countries and international organizations by the controller or processor".[13]

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

In these cases, the responsible entity may decide whether or not a third country or international organization offers an adequate level of data protection. Due to this there is a legal certainty and uniformity within the EU for a respective third country or international organization in cases where the Commission considers that the appropriate level of adequacy exists. In the event of a favorable decision from the Commission, personal data transfers may then be carried out without the need for further authorization.

After assessing the adequacy concerning the level of protection, the Commission may decide by means of implementing an act stating that a 3rd party country, territory or one or more specific sectors of a third county, or an international organization, will ensure the necessary and adequate level of protection. If no decision has been made, data controllers or processors may only transfer personal data to a third country or an international organization if they have assured the appropriate safeguards and provided that the data subjects have enforceable rights and effective legal and corrective remedies in place.

In the event that there is no decision taken on the appropriate level of protection, the controller or processor will take the necessary measures to remedy the inadequacy of data protection in the third part country by providing the appropriate guarantees to the data subject.

The provision for derogations from the lack of suitability decision or adequate guarantees is outlined in Article 49 within the GDPR. The individual's consent to the transfer of data according to Article 49 (a) should thusly be provided, "if the data subject has explicitly given their consent to the intended transfer, he has been informed of the possible risks of such transfers due to the lack of a suitability decision and adequate safeguards."[13]

Provisions should also be considered for situations where the transfer of data is necessary for the "conclusion or performance of a contract concluded between the data subject and the controller" or a contract "concluded in the interest of the data subject and the controller" or a contract "concluded in the interest of the data subject between the responsible entity regarding its treatment of another natural or legal person."

A decision known as the Safe Harbor Decision was adopted in July 2000 to provide an adequate level of protection for transfer of European Union personal data to organizations located in the United States. According to this decision, a personal data flow was allowed between the EU states and the United States under the Safe Harbor Decision. Safe Habour was invalidated after the Scherms case, a case where a citizen from EU considered his rights violated under the decision. The CJEU that the Safe Harbor didn't indeed offers an adequate level of data protection in the eyes of EU law.[17]

Following the declaration of invalidity of the Safe Harbor Decision, the European Union and the United States began to negotiate a new document in order to ensure the adequate level of protection regarding the transfer of data from the EU to the US, which would become known as the Privacy Shield. The emergence of this document would become a serious problem for several companies as well as also affecting Cloud Service Providers.

The Privacy Shield intends to reflect the requirements established by the CJEU within the Schrems case. The purpose of this framework intends to provide companies on either side of the Atlantic with a means of meeting the requirements regarding data protection adequacy when transferring personal data from the EU and Switzerland to the US. On July 12th 2016, the European Commission considered the Privacy Shield adequate to allow for data transfers under EU law. On January 12th 2017, the Swiss government announced the approval of the Swiss-US Privacy Shield Framework as a valid legal mechanism which meets Swiss requirements regarding the transfer of personal data from Switzerland to the US [19].

The Privacy Shield has been considered to be the most adequate in regards to adhering to data protection and transfer laws; however, it would still have to undergo several changes since its initial emergence to more thoroughly satisfy data protection regulations. This thesis will discuss these alterations in greater detail as well as their implications.

IX. CONCLUSION

The new digital era has led to an exponential exchange of data and personal information. Countries have long been concerned about the protection of

Extended Abstract: The new paradigm of Data Protection and the Impact on Cloud Computing

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

information with a special emphasis on personal data. The goal of this thesis is to focus on the contextualization of all the legislation surrounding the protection on data within the European Union. Meanwhile, with a greater focus on legislation being increasingly focused on the protection of individual data, the phenomenon of the cloud has become prevalent within our homes, businesses and the lives of all individuals. Additionally, there is the constant risk that whenever data is transferred from the European Union, the data subject may not be able to exercise their respective rights concerning their own personal information.

This thesis aims to focus on the impact of the General Data Protection Regulation of personal information within the cloud. This is especially relevant when it comes to deciphering the responsibilities of the Cloud Service Providers and that these respective responsibilities may vary depending on whether or not they are seen as a processor or data controller.

Until the emergence of the cloud, regulations focused solely on the responsibilities of the data controller, but new regulations have brought an entirely new perspective to light regarding the responsibilities of the processors.

An analysis is also expanded on within this thesis regarding the existing case law within the scope of transatlantic data transfers. It was found out that at the time of the Safe Harbor Decision that the supervisory authorities were not able to follow through on any complaints or investigations that were not within their possession or territorial scope. Although the emergence of the Privacy Shield framework, which has since been considered the closest to satisfying current data protection and transfer regulations, and although not flawless, is an example of the greater importance and governmental pressure being placed on protecting the data rights of individuals, it is concluded that there must be greater cooperation with supervisory authorities to uphold and honor the rights of individuals and their right to data protection in regards to actively altering and reexamining the laws in place alongside the evolution of new technological advances.

REFERENCES

[1] MELL Peter, GRANCE Timothy. “The NIST Definition of Cloud Computing”

[2] Fred Cohen & Associates A Short History of Cryptography

[3] Universal Declaration on Human Rights, adopted by the United Nations General Assembly, December 10th, 1948

[4] Spanish Constitution, Article 18 "1. “The right to honor, personal and family privacy and self-image is guaranteed”.

[5] Austrian Constitution, Article 10. "The privacy of letters may not be infringed and seizure of letters may, except in case of legal detention or domiciliary visit, take place only in times ofwar or by reason of a judicial warrant in conformity with existing laws”.

[6] Resolution (73) 22 On The Protection Of The Privacy Of Individuals Vis-A-Vis Electronic Data Banks In The Private Sector

[7] Resolution (74) 29 on the Protection ofthe Privacy of Individuals Vis-À-Vis Electronic Data Banksin the Public Sector

[8] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe

[9] “História da computação em nuvem: como surgiu a cloud computing?”

[10] IBM, “what is Cloud Computing”.

[11] KAI Hwang, GEOFFREY Fox, DONGARRA Jack, “Distribuited and Cloud Computing: from Parallel Processingg to the Internet of Things

[12] BUYYA, BRIBERG, GOSCINKI “Cloud *computing: principles and paradigms”,* John Wiley & Sons, Inc 2011 p.15

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[14] Constitution of the Portuguese Republic Article 26.

[15] Communication of Viviane Reding -The EU Data Protection Reform 2012: Making Europe the Standard

Extended Abstract: The new paradigm of Data Protection and the Impact on Cloud Computing

Catia S. Guerreiro Dionísio
Departamento de Engenharia Informática
Instituto Superior Técnico

Advisors: Prof. Doutor Carlos Caleiro & Prof. Doutor Alexandre Sousa Pinheiro

Setter for Modern Data Protection Rules in the Digital Age

[16] Eupean Comission “What is a data controller or a data processor?”

[17] Judgment of the Court (Grand Chamber) of 6 October 2015.
Maximillian Schrems v Data Protection Commissioner. Request for a preliminary ruling from the High Court (Ireland).
Reference for a preliminary ruling — Personal data — Protection of individuals with regard to the processing of such data — Charter of Fundamental Rights of the European Union — Articles 7, 8 and 47 — Directive 95/46/EC — Articles 25 and 28 — Transfer of personal data to third countries — Decision 2000/520/EC — Transfer of personal data to the United States — Inadequate level of protection — Validity — Complaint by an individual whose data has been transferred from the European Union to the United States — Powers of the national supervisory authorities. Case C-362/14.

[18] Report From the Commission to the European Parliament and the Council on the First Annual Review of the Functioning of the EU–U.S