Barros, Inocencio
Alvarez, Isabel

Data protection in cloud computing : a comparative study between the EU and USA regulations

http://hdl.handle.net/11067/7366
https://doi.org/10.34628/v4ms-4s57

Metadados

Data de Publicação 2023

Resumo In recent years, cloud computing has evolved a lot, but at the same time, threats have increased because data is accessed over the Internet. As most data centers are outside the European Union (EU) and are located mainly in the United States of America (USA), the researcher thoroughly studied the data protection laws that apply in both geographic areas. The subject of this study is based on the collection of necessary information and comparison of how personal data is handled in the European Uni...

Tipo bookPart

Editora Universidade Lusíada Editora

Data protection in cloud computing – A comparative study between the EU and the USA regulations

DOI: https://doi.org/10.34628/v4ms-4s57

Inocencio Barros[1], Isabel Alvarez[2]

[1] ISTEC
inocenciobarros1@my.istec.pt

[2] COMEGI, ISTEC, Autónoma TECHLAB
alvarez@edu.ulusiada.pt

Abstract. In recent years, cloud computing has evolved a lot, but at the same time, threats have increased because data is accessed over the Internet. As most data centers are outside the European Union (EU) and are located mainly in the United States of America (USA), the researcher thoroughly studied the data protection laws that apply in both geographic areas. The subject of this study is based on the collection of necessary information and comparison of how personal data is handled in the European Union (EU) and the United States of America (USA). In the EU, the study focused on the GDPR deepening the collection of information on the rights of data subjects, Basic Principles of Processing, Processing of Personal Data, Principle of Privacy for Data Protection, Organizational Requirements and then Legal Justification for Data Processing, while in the USA, by having a completely different approach that in the EU we addressed the CCPA and CDPA in-depth and WPA and NYPA superficially. First, the study focuses on the form of collection, processing, transfer, violation, and prevention of access of unauthorized persons. Then, a direct comparison between the GDPR and the CCPA was made, addressing data subjects rights, who is protected, the information protected and regulated by the entities. After making the comparison between the GDPR

and the CCPA, an interconnection was also made between the results of the previous comparison with cloud computing, with new responsibilities for CSPs as Processor, Customers or Supplier as Controller, Storage and Processing Policies, Data Subject Consent for Cloud Services, Security and Breach, Location, Transfer and Disposal of Data.

Keywords: Cloud computing; Data privacy; GDPR; CCPA; CDPA.

1. Introduction

1.1. The Purpose of the Research

Today, cloud computing is considered the latest computing paradigm that offers numerous consistent and flexible services using virtualisation technology that is used in next generation data centres. Not only private companies and individuals, but also government departments are increasing availability service through cloud computing infrastructures. Through its capacity, resilience and cost minimisation that provides the ability to share resources comprehensively and transparently, cloud computing also has the ability to perform procedures that meet different needs [5].

Today, most transactions take place online. The entities that manage these applications will have to comply with the new legislation, which protects the data of European citizens inside or outside the European Union (EU) [10]. The way we expose our personal data on the Internet, whether on social networks or on any other website where we carry out our transactions, requires some care, because we do not know where the data is stored and what the person on the other side can do with that data.

The United States of America (USA) followed the same steps as the EU, but slightly differently when it comes to data privacy applied to natural or legal persons [14]. In the USA, each state has its own entity to regulate the data privacy of their citizens. The state of California was among the first ones to pass the regulation, and follows the same laws as the GDPR on the rights and protection of Californian Citizen Data [14].

1.2. Scope and objectives

The main focus of this article is on the concerns raised about data privacy in institutions using cloud computing, which requires a rather rigorous investigation about the privacy of data of companies' customers in general. However, when using data in the cloud, one has to take into account the ethical and regulatory considerations related to data ownership. Existing legislation prevents institutions from processing, using the cloud in parts because of the way data management functions are defined at present and also because of the restrictions imposed by current rules.

1.3 Contributions to the research

The main contributions of this research are to provide an understanding of data privacy, and how data can be processed by the EU General Data Protection Regulation; to explain how data privacy is applied in the United States of America which is completely different from the European Union; through comparative methodology, the way data privacy is applied in the USA and Europe was compared. Information was gathered on data privacy in the EU, the USA and their privacy authorities, and finally, cloud computing and data privacy were linked to ensure compliance with the authorities regulating the processing of personal data in the two regions.

2. Literature Review

2.1. Cloud Computing

Cloud computing, is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction [13]. Cloud computing is defined as a set of computing services including servers, storage, databases, networking, software, analytics and intelligence over the internet (the cloud) to deliver faster innovation, flexible resources and economies of scale, where you pay only for the services you use in the cloud, reducing your costs in operations, manage infrastructure more efficiently, and scale as the business needs change [8].

2.2. Data privacy in the EU

The General Data Protection Regulation (GDPR), is a piece of legislation of the European Union, which protects and regulates the improper processing of data, of all European citizens. The intention is to bring more and better transparency, to the processing of an individual's data and boost the digital economy of member and participating states [7].

2.3. Data privacy in the USA

The United States of America have a different approach to personal data protection laws applicable to private companies. With the exception of industry-specific federal statutes, most data protection regulations applicable to businesses originate in the state. Reasonableness is determined by balancing two important interests: first, the intrusion on an individual's Fourth Amendment rights, and second, the government's legitimate interest in public safety [1]. There are some USA federal laws that recog-

nise privacy and data protection rights outside of the Fourth Amendment. However, these laws are generally limited in scope to specific sectors.

2.4. Privacy and Protection Laws in the USA

2.4.1. California Consumer Privacy Act — CCPA

It is the most comprehensive statute in the United States on data privacy law, after expected amendments; this new law came into force in January 2020 and applies to any company that meets one of the following thresholds [14, 3]: Gross annual revenues of $25 million; Obtains personal information from 50,000 or more California residents, households or devices annually; Fifty percent or more annual revenues processing personal information of California residents [15, 14]. Based on the GDPR, the California Consumer Protection Act (CCPA), was signed into law on June 28, 2018, and went into effect on January 1, 2020; it provides California residents with a number of rights, including the right to know what personal data is collected and how it is shared [14], exclude data sales from a company, and compel a company to delete important data.

2.4.2. Washington Privacy Act — WPA

Under the law, Washington residents are entitled to access categories of information processed about them, correct inaccuracies, suppression of the request, receive their personal information collected, exclude the processing of information for, among other purposes, targeted advertising and third-party sales [14]. However, compared to the CCPA, the WPA reduces the boundary of businesses that fall within the statute's purview. The WPA limits the ability of Washington residents to recover for violations; unlike the CCPA, the WPA does not provide a private action for Washington residents.

2.4.3. New York Privacy Act — NYPA

Broader in scope than the CCPA and WPA, the NYPA does not define the term business, and lacks a higher revenue or consumption threshold than would expose businesses to liability. Unlike the GDPR, CCPA and WPA, the NYPA contains a clause setting out the duty of care, which companies owe to consumers about the maintenance of their data [14]. The clause states that companies must act in the best interests of the consumer, regardless of the interests of the entity, the controller or the data broker.

2.4.4. Virginia Consumer Data Protection Act - CDPA

The CDPA shares common features with the California Privacy Act and state privacy bills, but also contains its own unique requirements. As a result of these unique requirements, companies subject to the CDPA, to take effect on January 1, 2023, will need to take specific steps, to ensure that their data processing complies with it [12]. The CDPA applies to businesses operating or manufacturing in Virginia or services marketed to Virginia residents.

3. Methodology and methods used

Initially, a systematic literature review [9] was conducted to identify, select and investigate the most relevant articles related to the themes of this research for the description and explanation of the situation under study. Subsequently, a comparative study [2] was conducted to explain the similarities and differences, between the data researched on the situation found in the EU and the USA, deducing their similarities and differences.

4. Data Privacy in the EU versus the USA

Cultural differences between the USA and the EU regarding privacy rights and data protection means that USA companies may have difficulty understanding and implementing the GDPR [1]. The fact that USA citizens do not have general data privacy rights and protections enshrined in the Constitution or federal statute, results in companies, at least initially, treating data differently in the USA compared to the EU [1]. There is a difference between the laws: it is that most USA privacy laws, including the CCPA, only protect the privacy of residents, while the GDPR and the Personal Data Protection Act in the EU, regulate any processing of personal data in local territories, including personal data relating to persons residing in other countries [4].

4.1. Restrictions on Data Collection and Ensuring Accurate Data

4.1.1. EU

The GDPR is a much more comprehensive piece of legislation than the Americans' counterpart; it begins regulating data protection before the data subject provides their information to the covered entity, and continues its regulation through the processing and storage phase, until the protected information is deleted [10]. Data is collected only for explicit and legitimate purposes, and must be limited to what is necessary for that purpose; in addition to this, the GDPR requires each data subject to give

their consent freely, to store their personal data and revoke consent to the storage or processing of their personal information [10]. The GDPR also imposes additional restrictions on the collection of certain types of data, including racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership and data concerning health or sexual orientation [10].

4.1.2. USA

In the USA, current law limits data collection, like data protection law in general, and is an attempt to regulate data collection in certain areas. For example, for medical information, the Health Insurance Portability and Accountability Act (HIPAA) requires that the data subject be given the opportunity to object, although silence equals consent, to the entity storing the data subject's name, location, etc.

4.2. Data Processing/Treatment Restrictions

In the EU data processing, refers to how the data collected is to be used once it has been collected; the GDPR defines a processor separately as a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller. A processor may also be the same entity that collects the data. If the entities (companies that handle or process the data) are the same, the processor is limited to using the data only for the reasons specified in the contract between the collecting entity and the specified processor. The GDPR explicitly defines processing, as a separate stage of the data protection cycle and addresses it individually, by requiring a data subject's consent for their data to be processed. The data subject must be informed about the purpose of the collection, how they will be used and processed prior to collection, and the data subject's consent must be freely given, specific, informed and unambiguous [10].

In the United States of America there are no specific limits on processing under current law, and data processing appears to be a mostly self-regulated area; most people who have the option to choose whether or not to provide their information have only an idea of how the data will be used. Processing limitations would be most useful in circumstances where the processing is not immediately obvious to the data subject, such as for further marketing and sale of information to other entities [10].

4.3. Data Transfer Restrictions

In the EU, data protection legislation must balance the needs of commerce, which benefits from open data transfers, with the privacy and security needs of the data sub-

ject, who benefits from minimal data transfers. The GDPR focuses primarily on the transfer of information outside the European Union, to entities not covered.

In the USA, regulations also place significant emphasis on limiting information transfers, in a number of different regulations; In both European and USA law, much of the focus in data protection rules concerns the transfer of data.

4.4. Breach and Prevention of Unauthorised Access

In the EU the first step in preventing unauthorised access to personal information, is to determine the risk of access attempts and what risks unauthorised access would pose to a data subject. Under the GDPR, a data protection impact assessment is particularly necessary where automated processing could produce a legal effect on a person; the processing is on a large scale and involves the special types of information described above.

In the USA, data protection laws take a more generalised approach to breaches; covered entities must then act on that risk assessment by implementing security measures to reduce risks to a reasonable level, sanctioning employees who do not meet security policy requirements and implementing ways to review data storage system activity [10].

5. Comparison between EU [GDPR] and USA [CCPA]

There are differences in the view of privacy rights and data protections in the USA and the EU [1]. Europeans operate from the perspective that customers own their data, whereas USA companies see themselves as owning the data because they are either the employers or the ones who have spent millions (or billions) to collect and analyse that data. Privacy and data protection are two rights enshrined in the EU Treaties and the EU Charter of Fundamental Rights. The EU has elevated data privacy to the domain of individual rights and protected these rights through the General Data Protection Regulation. Unlike the EU, in the US there is no individual right to data privacy and or data protection enshrined in the US Constitution [1].

The Fourth Amendment, does not provide a constitutional right to privacy; instead, it protects individual privacy from certain types of government intrusions, in other words, the Fourth Amendment protects people from unreasonable government searches and seizures, but does not guarantee a general right to privacy [1]. Table 1 was derived from the source obtained in the work of Jehl & Friel [6].

6. Data Privacy (EU) in relation to Cloud Computing

To comply with the GDPR, cloud services that regularly manage data, should be designed to address privacy concerns (privacy by design), allow processing of only the data that is absolutely necessary for system operations, and limit access to the data to only individuals involved in the processing. Policies and tools had to be put in place, to give data subjects the right to transfer their personal data to other providers, and to delete their data when they no longer need to be processed [11]. PaaS offers a development and deployment environment in the cloud, representing the operating system layer. However, the customer has no direct control over the execution environment and logging and encryption mechanisms can be implemented on the platform, so that providers can collect and store data, to be used by the customer for different purposes, such as security checks [1]. In terms of data processing, SaaS and IaaS technologies are at ends of the same scale, so their providers have different responsibilities and roles. An IaaS provider typically offers a software application service that is specifically intended to process personal data. A SaaS provider can exercise a wider range of controls over data processed using its SaaS [11]. As the GDPR covers all entities that store, process or transfer data in the European Union, as well as those that store, process or transfer data relating to persons residing in the European Union or where the laws of European Union Member States apply, all covered entities are held to the same standards [10].

Table 1 EU vs US Comparison Score, source [6]

The Rights	USA - CCPA	EU - GDPR	Comparison
Data Portability	In response to a request for disclosure, a company must provide personal information in an easily usable format to allow a consumer to transmit the information from one entity to another entity without hindrance.	It includes a new right to data portability, to receive a copy of personal data in a structured, commonly used and machine-readable format, and also to transmit personal data to another data controller	Similar rights, the GDPR provides a specific right to request a data controller to transfer your personal data, to another data controller.
Disposal (to be forgotten)	A consumer has the right to delete personal information that a company has collected, subject to certain exceptions. The company must also instruct its service providers to delete the data.	Data subjects, have the right to request the erasure of personal data in six circumstances (the right to be forgotten). Data controllers, must also take reasonable steps to inform any other data controllers, who also process the data.	Similar data erasure rights. The GDPR right only applies if the request meets one of six specific conditions while the CCPA right is broad.

The Rights	USA - CCPA	EU - GDPR	Comparison
Correction	None	Gives data subjects the right to: correct personal data when they are incomplete.	Substantially different.
Restricting Processing	None, other than the right to exclude the sale of personal information.	Right to restrict the processing of personal data under certain circumstances.	Substantially different.
Subject to processing	None, other than the right to exclude the sale of personal information.	Right to object to processing for profiling, direct marketing and statistical, scientific or historical purposes.	Substantially different.
Exclude for sale personal information	Businesses should allow and comply with a consumer's request to opt out of the sale of personal information to third parties, subject to certain defences. Must include a "Do not sell my personal information" link in a clear and visible location on a website homepage.	It does not include a specific right to exclude sales of personal data. However, the GDPR does contain other rights that a data subject may use to achieve a similar result in certain circumstances.	Substantially different.
Who gets regulated?	Any business in California that meets one of the following: has gross revenues exceeding $25 million. Annually buys, receives, sells or shares the personal information of more than 50,000 consumers, families or devices for commercial purposes. Obtains 50% or more of its annual revenue from the sale of consumers' personal information.	Processor or Data Controller: in the EU process personal data in the context of activities of the EU establishment, regardless of whether data processing takes place in the EU. Processing personal data of an individual outside the EU, concerns the offering of goods or services in the EU.	The territorial scope of the GDPR is much broader. Substantially different

The Rights	USA - CCPA	EU - GDPR	Comparison
Who is protected?	California resident consumers. Consumers include: customers of household goods and services. Employees. Business-to--business transactions	Data subjects, defined as identified or identifiable persons to whom the personal data relate.	Substantially different in approach, but equally broad in effect. Both laws focus on information relating to an identifiable natural person, however the definitions differ.
Which information is protected?	Personal information that identifies, relates to, is capable of being associated with, or could reasonably be linked, directly or indirectly, to a particular consumer or household	Personal data is any information relating to an identified or identifiable data subject. The GDPR prohibits the processing of defined special categories of personal data, unless a legal justification for the processing applies.	Substantially similar. However, the CCPA definition also includes information linked to the level of the household or device.

7. Major findings

With the information gathered on cloud computing, it can be observed that this technology plays a very important role in the way small companies survive in comparison to large companies, starting with the numerous services made available. But the focus of this dissertation is centred on security and privacy, which are points that companies have in common and continue to be a concern for both companies and cloud providers. As data is accessed over the Internet, the threat to data integrity is greater, because it is more exposed to attacks by hackers or malicious people, so both the customer and the cloud provider have shared responsibility in this field, depending on the type of service that companies contract.

In the study done on how personal data is handled in the EU and the USA, it was noted that despite the efforts of the North Americans, there is still a long way to go to match Europe. It is known that in the USA the approach to data privacy is different compared to the EU. In the EU, there is only one entity to regulate how European citizens' data is handled inside or outside the EU, while in the US each state has its own entity to deal with data privacy. However, there are commonalities, such as, for example, both entities uphold the right of data subjects, even though the definition is substantially different.

8. Conclusion

The comparison made between RGPD and CCPA [see Table 1 above], regarding who is protected and the information to be protected, leads us to the conclusion that both entities have these two points in common, but with a slightly different approach from each other. It can also be observed that both focus on information related to an identifiable natural person, but differ in the definitions. Both have potential extraterritorial effects that companies located outside the jurisdiction should consider; however, the CCPA definition also includes information linked to the household level. To comply with privacy laws, new responsibilities have been created for cloud providers, either as processor or controller of the data in the cloud. Previously, SaaS was the only service model for handling and processing customer data; now, new responsibilities have been created for IaaS and PaaS. The study produced reveals that despite the efforts of cloud providers, there is still a long way to go when it comes to security and privacy, starting with the part where data is accessed over the internet.

References

1. Barrett, C. (2019). (S. Lawyer, Ed.) Are the EU, GDPR AND the California CCPA becoming the de Facto Global Standards for Data Privacy and Protection?, 15(3)
2. Fachin, O. (2001). Fundamentos de metodologia. São Paulo: Saraiva
3. Goldman, P. E. (2020). An Introduction to the California Consumer Privacy Act (CCPA). An Introduction to the California Consumer Privacy Act (CCPA), pp. 2-5
4. Gupta, L. D. (2019). India's Personal Data Protection Act, 2018: Comparison with the General Data Protection Regulation and the California Consumer Privacy Act of 2018. Berkeley Journal of International Law, 37(3), 24-32
5. Issi, H. N., & Ef, A. (2018). Cryptography Challenges of Cloud Computing For E-Government Services. International Journal of Innovative Engineering Applications, 2(1), 1-2
6. Jehl, L., Friel, A., & LLP, B. (2018). CCPA and GDPR Comparison Chart. A Chart comparing some of the key requirements of the California Consumer Privacy Act (CCPA) and the EU General Data Protection Regulation (GDPR)., pp. 1-8
7. Mammona, A. N., Kanwal, N., Fleury, M., Herbst, M., & Qiao, Y. (2019). Visual Surveillance Within the EU General Data Protection Regulation: A Technology Perspective

8. Microsoft. (22 de July de 2021). Microsoft. (Micorsoft Corporate) Obtido em 22 de July de 2021, de Microsoft Azure : https://azure.microsoft.com/en-us/overview/what-is-cloud-computing/

9. Okoli, C., (2015) “A Guide to Conducting a Standalone Systematic Literature Review” Communications of the Association for Information Systems, Vpl. 37, Article 4

10. Peasley, M. (2019). It’s Time For an American (Data Protection) Revolution. Akron Law Review, 52(3), 7-20, 28-29

11. Russo, B., Valle, L., Bonzagni, G., Locatello, D., Pancaldi, M., & Tosi, D. (2018). Cloud Computing and the New EU General Data New EU General Data. IEEE Computing Society, 3-7

12. Simmons, M. R. (2021). New Virginia Privacy Law Promises Big Impacts. The Computer & Internet Lawyer, 38(6)

13. Taghipour, M., Mowloodi, E. S., Mahboobi, M., & Abdi, J. (2020). Application of Cloud Computing in System Management in Order to Control the Process. 3(3), pp. 3-4

14. Ventura, L. (2020). “Senator, We Run Ads”: Advocating for a US Self-Regulatory Response to the EU General Data Protection Regulation. (S. C. Ondrof, Ed.) 28(2)

15. Voss, G. W., & Houser, K. A. (2019). Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies. p. 9