IPASJ International Journal of Computer Science (IIJCS)
Web Site: http://www.ipasj.org/IIJCS/IIJCS.htm
A Publisher for Research Motivation ..... Email:editoriijcs@ipasj.org
Volume 5, Issue 7, July 2017 ISSN 2321-5992

The implication and challenges of GDPR's on Cloud Computing Industry

Sohail Razi Khan[1], Professor Luis Borges Gouvia[2]

[1]Sohail Razi Khan, University of Fernando Pessoa, Porto, Portugal

[2]Professor Luis Borges Gouvia, University of Fernando Pessoa, Porto, Portugal

Abstract

The European Union (EU) existing Data Protection Legislation has become obsolete as it doesn't cater the new developments in-terms of high use of social networking platforms, explosion in the growth of data and emergence of the cloud computing technology. There was an urgent requirement to revamp the existing Data Protection Directive by General Data Protection Regulation which will have serious implications on all sectors of the value chain including the cloud service providers. This research paper is an attempt to explain the journey and need to move towards the new data protection regulation. The paper explains the implication of the General Data Protection Regulation on the cloud service providers and how it will impact the processes of the cloud service providers. Findings of the paper can assist the cloud service provider to overhaul their processes and procedures to meet the challenges that will affect their operation due to the implementation of the law.

Keywords – General Data Protection Regulation (GDPR), Cloud Service Provider (CSP), Data Protection Directive (DPD), European Union (EU), Data Protection Agency (DPA)

1. Introduction

The ever-changing requirements of the business world with new rights for individuals and recent news related to data security breaches there is no ambiguity that the European Union General Data Protection Regulation ('GDPR') will have serious implications on cloud service providers, process and storage of personal data. The cloud providers need to integrate this new law into their processes and make rectifications accordingly to meet the new provisions. The European Union (EU) existing Data Protection Legislation [1] is becoming obsolete as it doesn't cater the new developments in-terms of high use of social networks, exponential growth of data and large scale usage of cloud computing technology. Using cloud computing is an integral part for a modern business to operate nowadays because it can provide competitive advantage by reducing cost and allowing small sized companies to compete with large multinational companies without high startup costs. According to International Data Corporation (IDC, 2016), forecast more than 80% of new commercial enterprise applications will be using cloud as platform by 2020. EU commission understand the importance of cloud computing and desire to adapt cloud friendly policies that can generate 250 billion Euro in GDP by 2020 [2]. This will result in substantial growth in the job market by producing 3.8 million cloud-based jobs with proper policies and laws that provide suitable environment for cloud market.

The major hurdle in the use of cloud computing in Europe is the existing data protection legislation. The existing laws were not comprehensive as it provided member states an option to implement only minimum standards and due to this it is resulted into poor data protection standards and created more uncertainty in the adoption of cloud technology [2]. The implication of the General Data Protection Regulation (GDPR) is far reaching and cloud providers need to change and modify their services, processes, and contracts to meet the requirements of new legislation. The research paper initially discuss the transformation journey and underlying causes to enhance the Data Protection Directive (DPD) to General Data Protection Regulation (GDPR). The next section of the research paper highlight the new provisions in the General Data Protection Regulation (GDPR) and their impact on the cloud service providers, followed by a comparison between the current Data Protection Directive and changes in the GDPR. The research paper will summarize the legal and overall impact of GDPR on Cloud Service Provider (CSP) and how it will affect the processes and procedures while processing or storing data.

2. Set the Context: A Brief Literature Review

The new framework proposed in-terms of General Data Protection Regulation (GDPR), provides a comprehensive and uniform legal structure to provide a 'Digital Single Market' that ensures innovation, financial growth and safeguard the personal data. It ensures the ease in the movement of data within the European Union and also provide legal framework and protection for handling data by countries outside the union [3]. The European Commission proposed a

comprehensive legislation in the form of General Data Protection Regulation that will remove all ambiguity and form a single European data protection law that all members' states have to follow. The law follows the basic principles of Data Protection Directive [4], that secures the rights of the data subjects with more control over their data, proposes tough sanction for any data breaches and it is applicable to foreign companies and cloud service providers that are handling data of EU residents [5]. The new law bring a sea change in how organization must protect personal data for non-EU resident as well so it can be known as 'Global' Data Protection Regulation, as the law imposes serious financial penalties due to non-compliance, data breaches or poor security and privacy standards [6]. According to the law it is mandatory to notify any breach, ensuring the right to be forgotten and equally sharing the responsibility on the data controller and data processor which are crucial for protecting personal data. The cloud service providers has to review all the processes to understand fully the implication of GDPR as it requires both organizational and technological measures in response [7]. In the following section of the paper explains the transformational journey from Data Protection Legislation to General Data Protection Regulation in the context of new technologies such as cloud computing.

2.1.Data Protection Law: Transformation Journey in context of Cloud Technology

The existing EU Data Protection Directive provides a legal framework for data protection in the European Union. When the law was passed in 1995 it provided a comprehensive mechanism for data protection at that time. The major change was introduced in the form of Treaty of Lisbon in December 2009 by which the data protection was given the status of fundamental right [8]. The DPD law was not equipped to manage the explosion of data we have observed in the recent past due to social networking and high use and demand of cloud computing technology for storage and processing of large amount of data [9]. The existing law was not able to answer questions such as data storage using cloud technology; where the data can be stored on a third party servers which the owner will have no access to it. The other deficiency of DPD was failed to produce a uniform approach to data protection in the EU as there was different interpretation of law by member states and ambiguous standards for data protection rules were applied by these member states in the EU [10]. This huge disparity has resulted in confusion and costly administrative burden for businesses operating in the member states. The confusion that was created due to weakness of DPD can be considered as a major barrier to the adoption of cloud technology in EU.

There was huge outcry after Snowden revelations of unauthorized surveillance which has forced to reform the entire data protection structure. With the integration of 'digital agenda' in the economy, use of social platforms and cloud technology there is explosion in data generation and the existing data protection laws were considered as a huge barrier in the implementation of this agenda [11]. According to data protection working party, Article 29 Working Party (WP29) came with a list of recommendation how to integrate and use cloud computing technology as the concern were that massive use of cloud technology will lead to data at risk and with lack of control over data [12]. The development and use of cloud technology have highlighted the weaknesses and shortcomings in the existing Data Protection Directive as with the use of technology the data moves rapidly within the cloud infrastructure and there is lack of clarity on the physical location of data which is a matter of concern for the data owner. The majority of existing cloud computing contracts are restricted in the sense as they reduce the responsibility of cloud processor as compared to the potential risk for the data subjects [13].

The challenges of the new technology forced the European Commission (EC) to propose a new law that can address the shortcomings. In order to incorporate those changes, EC in 2009, announced that they have initiated a procedure for data protection reform, after detailed deliberation and discussion in April 2016 General Data Protection Regulation (GDPR, Regulation) was adopted [13] [14]. The law introduced significant changes after a detailed ruling in the case of 'Digital Rights Ireland', [15] that invalidates 2006 Data Retention Directives that requires private cloud provider to store and keep metadata for electronic communication for a long period of time for law enforcement purposes. The next significant change that was incorporated was the right to be forgotten. In the 'Google Spain case' [16], the court understood the right to be forgotten as fundamental right of the user. The other change in the law was seen by invalidating the Safe Harbour in Schrems [16], in which transfer of data between EU and US is not offering a level of data protection according to the standards of EU. The court also ruled that US intelligence services have access to this personal data which is comprising the fundamental rights of the EU citizens. The EU commission intended to advance and establish the use of cloud services in all the member states but at the same time reassure all the citizens that their personal data is safe and under their full control. The GDPR will ensure the data is protected from unlawful access and issues related to compliance are easier for all the cloud service providers operating in the EU. The law provides

encryption, extraterritoriality, and trans-border of data flow which will increase the standards of data protection according to the fundamental rights which will place the cloud service providers operating in the EU an advantage over the competitors in non-EU countries. This law has seen a transformational journey which incorporates the impact due to the use of advanced technology and can set direction by raising data protection standards for the global cloud market.

3. General Data Protection Regulation: New Provisions and impact on Cloud Service Providers

3.1.An Uniform Approach to Data Protection Laws in EU

The GDPR will provide a uniform approach to the data protection law in the all the member states in the EU by having a single set of rules on data protection across the union. The law will replace the existing inconsistent national data protection law that have created confusion and ambiguity [17]. The law will be immediately and at the same time will be implemented on all member states and the current Data Protection Directive will not be valid anymore [18]. This law will provide a uniform approach to the data protection and can't be changed or weaken by various member states at the national level. The massive legislative change is being welcomed by cloud service providers as it brings a uniform single data privacy law across the all the member states by reducing the operational cost and ensuring ease in compliance activities [18]. The will allow the providers to compete effectively and assist businesses to grow their operations. The cloud providers in EU can have a competitive advantage by incorporating these directions and improve the Quality of Service (QoS) and standards. Whereas the providers across the world have to incorporate all these changes into their processes and procedures.

3.2 Processer fully Accountable

In the existing Data Protection Directive, data controller is solely responsible and accountable to maintain the security and privacy of data whereas data processor carries no legal burden. According to the Directive rule data processors are processing data for data controllers and are not subject to data protection and security rules. There are serious implications of GDPR on data processor by including the processor in the ambit of rules now [19]. With the new law the processor are directly accountable for data processing so the cloud service provider CSP processes and operations will be affected. CSP can't avoid the accountability anymore and in order to incorporate the law have to further develop and implement number of internal procedures and practices to safeguard data. The problem that shouldn't be overlooked is the burden the law will create on the small size CSP processors.

3.3 Applicable to Non-EU Companies

With the implementation of GDPR it will extend the reach of territorial scope of the EU data protection law to all providers that processes personal data for the EU resident [20]. The existing DPD doesn't cover the situation where the controller is outside the EU and process personal data for EU customers [21]. The current DPD is quite inadequate, unclear and confusing dealing with the new technological advancements [22]. The GDPR removes any ambiguity that any organization that is based outside the EU that are processing personal data have to abide by the GDPR law and also will be held accountable. The cloud providers operating from outside the EU need to improve their processes and procedures to match the same Quality of Service (QoS) and standards offered by their competitors that resides in the EU.

3.4 Appointment of Data Protection Officer

The GDPR law stipulates a mandatory requirements for all companies and CSP to appoint Data Protection officers (DPO) to oversee the maintenance and security of the data. The law requires an appointment of DPO by the controller and the data processor where more than 5000 data subjects are being processed for more than 12 months in a period [23]. The core responsibility of DPO is to be independent and have professional qualities and expert knowledge to maintain the data protection law and ability to fulfill the responsibilities mentioned in the Article 37 [24]. The GDPR will enforce the processing of data by the controller or it can be processor that is based in any member states of the EU. The law is applicable to the processing of personal data of data subjects that are in EU by controller or processor that doesn't exist in the EU. This enforces an appointment of DPO to the data processor that doesn't exist in the EU. The implication of appointing the DPO is another financial burden on the CSP which will overall increase the customer's service fees.

3.5 Serious implications with Subcontracting

There are serious implications for CSP processor due to Article 26 that stipulates clearly processor without the advance written consent of the controller can't subcontract to the other processor [25]. So it is clear that any sub-contracting can only take place if advance consent is taken. The law allows an open consent to subcontracting to processing of data if agreed upfront. The law stipulates that CSP processor have to inform the data controller in-advance of any changes which will provide the opportunity to the data controller to stop any changes that can compromise the security or privacy of the data. The implications due to Article 26 will force the CSP to change their existing procedures and can create an operational burden for some providers.

3.6 Data Breach Notification

According to the GDPR it is essential to report any data breach to the concern stakeholders without any delay. The data controller has to inform the responsible supervisory authority in the EU [26]. The law stipulates that any data breach should be informed to the data subject with close cooperation with the supervisory authority. As soon as the organization is aware of the data breach they have 72-hours windows to notify the authority. The Article 33(3) [27] stipulates four requirements when reporting a data breach should be highlighted such as the notification within the reasonable time (72 Hours), the nature of personal data breach containing the categories of data and numbers of data subject records breached, provide the name and contact details of the data protection officer and explanation to the cause of the consequences of the data breach. This provision of the law will impact the existing processes and will require more resources in-terms of manpower to accommodate the new provision of the law.

3.7 Right to Data Portability

Data subject has full authority and right to request the data to be moved under the Article 20 of the law. The article states that the personal data that is stored with the controller can be moved to another controller upon the request of the data subject.

3.8 ONE-STOP Initiative

As per the GDPR all EU residents and different data processor and controllers will deal with only one DPA (Data Protection Agency) across the EU [27]. Different organizations in each member states will have a DPA in the country where they are established [28]. This will increase the uniformity and eliminate any ambiguity and ensure that all decisions are locally made [29]. This will allow CSPs to work closely with the DPA to improve the overall efficiency and enhance the protection of the data.

3.9 Serious Penalties for Negligence Breach

There are serious implications in-terms of financial penalties if there is a 'negligent breach' that leads to data and privacy loss. The law proposes a fine up to 5% of annual revenues and maximum fine up to 100 million euros [29]. There is new potential offence that can have serious consequences to the data breach is known 'Unjust Enrichment'. This is happened when the company save money and doesn't apply enough security measures to protect data which results in data security breaches. The EU commission is planning to incorporate this into law which will have serious implication of CSPs.

3.10 Right to be forgotten

The law clearly stipulates that if EU resident no longer want their data to be processed or store they can request the complete removal of data. The burden is on the organization to completely remove the data and don't keep any information about the specific user [30].

4. Comparison of DPD Vs GDPR

The GDPR will provide a uniform approach to the data protection law in the all the member states in the EU by having a single set of rules on data protection across the union. The law will replace the existing inconsistent national data protection law that have created confusion and ambiguity and proposes new provisions as seen from the following Table 1.1, that will improve data security and privacy but at the same time will have serious implications for CSPs and their procedures and processes.

Current Data Protection Directive 95/46/EC	Changes created by GDPR
European reach only	Global reach
Local law divergence across 28 EU states	Regulation: uniform across EU

Multiple Data Protection Authority ("DPA") Exposure	"One stop shop"
Limited Accountability	Accountability Key
Controllers Only	Controllers and Processors
Small fines, differ between countries	Huge fines
No obligation to report breaches	Obliged to report breaches without delay
No obligation to have DPO (Data Protection Officer)	DPO required for larger organization

Figure 1: Changes in existing EU Data Protection Law [28]

5. Final Remarks

The GDPR is one of the most powerful legislation which will have serious implications for cloud service providers and business that interact with the customers. The law is not only a compliance challenge but it will have impact on all sectors of the organization's value chain, affects data processor and data controllers operations. The CSPs have to overhaul their entire processes, revise how the personal data is stored and processed to ensure complete compliance that will add value and identify new ways to provide better customer service with complete data security. In order to implement all provisions of the GDPR, the CSPs should go for a thorough review of the entire organization security procedures and data protection standards and revise the roles and responsibilities. The re-examination of organization data stategy that is related to the personal and sensitive personal data should be initiated. Various requirements of the GDPR should be planned, organizational and technological approaches implemented to resolve problems and strengthen policies and procedure to reduce the worst outcomes. The data protection procedures must be designed by default and standards of CSP should be improved to meet the requirements of the law. The next major implication of the law is that non-EU firms have to make rapid changes as they will be subjected to EU data protection directive now. The new level playing field is introduced by the GDPR that is applicable to all firms regardless of their location if they are processing personal data related to EU residents. All the provisons of the law can be adapted if both the technological and organiational responses are in-place. With the use of advanced technologies such as cloud computing the compliance will be required from set of coordinated responses from the organization as a whole with strategy, policy, training and goverance processes needed to comply with GDPR. One potential issues with the GDPR rule is based on the binary assumption as there is only controller and processors. In the real world there are groups of companies buying services and have hosting facilities subcontracted across the globe. There is always uncertainty of new rules with the issue of non-compliance which exist while the implementation of the new law. It is evident that the new provisions introduced in the GDPR will improve the security and privacy of data but will have serious implications and challenges for CSPs.

References

1. 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, 1995 O.J. (L 281/31) ("Data Protection Directive"). IDC 2012, p. 48 – 64.
2. Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 STAN. J. INT'L L. 53, 68 (2014); Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S., 2012, at 109.
3. Eur. Comm'n, 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 free movement of such data, EUR. COMM'N DOC. (COM (2012) 11 final, Jan. 25, 2012) (General Data Protection Regulation – Initial Version of European Commission).
4. General Data Protection Regulation – Consolidated Version of LIBE, Recital (7); Andrej Savin, EU INTERNET LAW 206 (2013).
5. Press Release, Eur. Comm'n, Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author); Eur. Parl., Q&A on EU data protection reform (Mar. 4, 2014) http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protectionreform.
6. Dataguidance.com, Discussions on the Regulation are mature (Jan. 30, 2014), http://www.dataguidance.com/ dataguidance_ privacy_this_week.asp?id=2197.

7. Press Release, Eur. Comm'n,, Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).
8. Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community [2007] OJ C306/01.
9. See Commission, 'Data Protection' (2015) Special Eurobarometer 431/ Wave EB83.1
– TNS opinion & social, Summary, 2 <http://ec.europa.eu/public_opinion/archives/ebs/
ebs_431_sum_en.pdf> accessed 10 May 2016.
10. Eur. Parl., Q&A on EU data protection reform, http://www.europarl.europa.eu/news/de/news-room/content/20130502BKG07917/html/QA-on-EU-data-protection-reform (Mar. 4, 2014).

11. The Article 29 Working Party is set is up under the Directive 95/46/EC. It is composed of representatives from all EU Data Protection Authorities, the EDPS and the European Commission. It has advisory status and acts independently.
12. WP 29 Opinion 05/2012 on Cloud Computing, adopted on 1 July 2012.
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) [2016] OJ L119/1.
14. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland EU:C:2014:238.
15. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland EU:C:2014:238.
16. Case C-131/12 Google Spain and Google EU:C:2014:317.
17. Schrems (n 7)
18. Press Release, Eur.Comm'n., Progress on EU data protection reform now irreversible following European Parliament vote (Mar. 12, 2014) (on file with author).However, European Commission's decisions adopted and authorizations by supervisory authorities based on the Data Protection Directive should remain in force. See General Data Protection Regulation – Consolidated Version of LIBE, Recital (134).
19. TFEU Article 288 Section 2; Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 STAN. J. INT'L L. 53, 68 (2014).
20. Lukas Feiler, INFORMATION SECURITY LAW IN THE EU AND THE U.S. 109 (2012).
21. Id. See also Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 Stan. J. Int'l L. 53, 53 ff. (2014).
22. Andrej Savin, EU INTERNET LAW 197 (2013).
23. See also Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 STAN. J. INT'L L. 53, 65, 73, 100 (2014).
24. General Data Protection Regulation – Consolidated Version of LIBE, Recitals (19), (20); Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 STAN. J. INT'L L. 53, 71 (2014).
25. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union – Consolidated version of the Treaty on the Functioning of the European Union – Protocols – Annexes – Declarations annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon,signed on Dec. 13, 2007 – Tables of equivalences (Treaty on the Functioning of the European Union – TFEU),
26. Article 288 Section 3 2012 O.J. (C 326, Oct. 26, 2012 P. 0001 0390) ("TFEU"); Dan Jerker B. Svantesson, The Extraterritoriality of EU Data Privacy Law—Its Theoretical Justification and Its Practical Effect on U.S. Businesses, 50 STAN. J. INT'L L. 53, 68 (2014).
27. David Loshin, Sever Data Strategies for Regulatory Compliance :http//governyourdata.com/page/white-papers
28. Samuel Mischler, Synthetic data and its consequences, how to eliminate legal and regulatory obstacles in testing, SOS Whitepaper Book, 2014
29. In this regard, see M Brkan, 'The Unstoppable Expansion of EU Fundamental Right to Data Protection. Little Shop of Horrors?' (2016) 23(5) Maastricht Journal of European and Comparative Law 812
30. Jan Philipp Albrecht, "EU General Data Protection Regulation State of play and 10 main issues", The Greens/EFA in the European Parliament, 7 January 2015, www.janalbrecht.eu/fileadmin/material/Dokumente/Data_protection_state_of_play_10_points_010715.pdf, p. 3.
31. Summaries of EU legislation, "Subsidiarity", European Union, europa.eu/legislation_summaries/glossary/subsidiarity_en.htm, Accessed 28 May 2015.

32. Factsheet on the 'Right to be Forgotten' ruling (C-131/12)", European Commission, 2 June 2014, ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf, p. 3.

AUTHOR

Sohail Razi Khan received MSc (Distributed Networks and Security System) from University of Hertfordshire, M.A in (Education and Leadership) from University of Wolverhampton and MBA in (Business Administration) from University of Central Lancashire, from England. Mr. Khan is involved in teaching computer science in higher education institutions from last 12 years and currently pursuing his PHD (Doctor of Philosophy) in the field of Cloud computing and Data Security issues. Mr. Khan has worked as a IT strategy consultant providing advice and solutions for business enterprise as well.

Professor Luis Borges Gouvia has extensive experience in academics, monitoring various researches, publication of various books and contributed extensively in latest research in the field of cloud computing, cyber security, E-Commerce and Web 2.0 and Higher Education. Professor Gouvia, has PHD (Doctor of Philosophy), from University of Lancaster, England. He is a full professor in University of Fernando Pessoa, Porto, Portugal and successfully supervised various PHD students.