

## A comparative analysis between General Data Protection Regulations and California Consumer Privacy Act


Syed Khurram Hussain Naqvi<sup>1</sup>, Komal Batool<sup>2</sup>

<sup>1,2</sup>Riphah Institute of Systems Engineering, Riphah International University, Islamabad

### ABSTRACT

Data breach is a common phenomenon in these days. Entities holding the personal data are involved in providing data to marketing and other companies for their benefit. Consequently, the citizens suffer and pay the price of breaching. Various countries have adopted personal data protection laws in line with General Data Protection Regulations (GDPR). The California State has also made legislation to secure consumer rights in respect of personal data. This study made a comparison between General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). After study, it has been identified that GDPR is a comprehensive document which can be used for providing security of personal data around the world. It has all the relevant clauses/ Articles that can be used accordingly. Furthermore, being dynamic in nature it has the capability to become adoptable to new changes/ technologies. However, there is a need to expand the scope of the study and conduct a comparative analysis on the basis of geographical boundaries. The future directions may include the study of laws relating to personal data protection of various developing countries in the context of the GDPR.

**Keyword :** Data Privacy, Data Protection, User, Data Breach

 This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

#### **Corresponding Author:**

Syed Khurram Hussain Naqvi  
Department of Information Technology  
Riphah Institute of Systems Engineering,  
Riphah International University, Islamabad.  
Email : skhn00@gmail.com

#### **Article history:**

Received Jan 19, 2023  
Revised Feb 29, 2023  
Accepted Mar 15, 2023

### 1. INTRODUCTION

The state of California is committed to provide safeguards to its citizen by taking various legislative and regulatory measures. One of these measures is to enact law pertaining to Personal Data to avoid breach and unlawful use of personal data. Purpose of enacting such legislation/ regulations is to empower the general public by providing comprehensive law of Personal Data Protection in line with General Data Protection Regulations (GDPR). By ensuring these steps, the individual shall have the assurance of non-disclosure of his Personal data and availability of an appropriate forum whereby, complaint of breaches of data theft could be addressed.

To secure privacy of personal data a law was enacted through American Legislators and it is known as California Consumer Privacy Act (CCPA). Various clauses of this Act are linked with GDPR articles. Thus, it is considered the most compact and solid legislation in the domain of personal data protection in State of California. It was passed in 2018 and came into force from 1st January, 2020. The aim of enacting this law was to ensure the belief about fundamental human rights protection of citizens of California. The legislators were of the view that existing privacy should be made more secure by introducing accountability mechanism on the data holders. It includes the purpose of holding data by the companies and its onward transmission/ utilization in marketing purpose. Another striking aspect was to ensure analyzing and improving data systems.

GDPR on the other hand is a legislation in the form of Regulations, enacted by European Union for protection of data. One of the important aspects of GDPR is Personal Data Protection which includes, personal information of all kinds, i.e., name, address and phone number etc. The GDPR is applicable to all European Union member States. It covers rights regarding business and citizens related data. The clauses of GDPR are very comprehensive and easy to implement.

The aim of conducting this study is to identify and highlight various differences between the two legislations and device future course of action for subsequent research in the area of data privacy and protection for various countries.

## 2. LITERATURE REVIEW

The oldest record of data protection regulation can be traced in Europe in the era of 1970's. Later, Sweden adopted data Act for personal data protection and computing. In USA the Fair Information Practice Principles (FIPPs) emerged to address transparency, data transparency, use illegal breach, access and correction, data quality, and security in the digital space. However, Fips did not delivered to make much impact in the USA.

Georgiadis, G., et al. conducted a study to identify risks associated with big data analytics in respect of personal data protection. GDPR through its data protection impact assessment highlights various controls to mitigate risks. They conducted a systematic literature review, whereby, they applied thematic analysis on 159 articles to identify risks which lead to definition of 9 Privacy Touch Points (PTPs) that summaries the identified risks. These PTPs were than analyzed for methodologies of Privacy Impact Assessment (PIA). The researchers identified the future course of action regarding developing comprehensive study comprising of comparison of data protection laws of various countries in connection with articles of GDPR.

To analyze and find differences between the GDPR and Data Protection Directive from 1995, Skendžić, A. et al. conducted a study in Croatia where in it was found that personal data represent identifiers including network IP address, first and last name, MAC address, telephone number, GPS location, personal ID, biometric data and other relevant data in connection with personal identity. It was also found that GDPR is the harmonization of business operations with legislation enforced at state level. Moreover, Synchronization of Court of Justice and GDPR articles is also necessary. Organizations are also find 0.5 to 4% of the global annual turnover or upto 20 million Euro, if found non-compliant to GDPR. It was also narrated that GDPR would be working under Croatian Personal Data Protection Agency and actions will be taken under the authorized direction of the agency. Various rights including Forgotten Rights were also insured. Finally, it is concluded that the data of legal persons, or entrepreneurs as legal persons does not come under the purview of GDPR.

Grundstrom, C., et al. studied the area of data access research it was found that very little is available about how to access personal data in respect of insurance organizations. In this regard compliance challenges i.e. Proliferation, Protection, Procedure and Privacy after qualitative analysis of insurance companies 13 challenges of GDPR compliance were identified related to the four categories. However, certain limitations were associated with this research. Firstly, the study was based on specific industry i.e. insurance, thus, the scope of study was very limited. It was suggested that empirical studies with widened scope should be carried out while considering the compliance of GDPR in respect of personal data access. It was further pointed out that the area of personal data access should also be exploited country wise and region wise.

A study was conducted by Papaioannou, G., et al. to correlate the articles of GDPR with Big personal data in terms of memory institutions and cultural heritage as handlers. The focus of the study was to identify common risk factors while implementing the regulations of GDPR. It was admitted that the advent of GDPR has become a certainty and once its regulations are enforced it would be a binding effect on the organizations. Therefore, the organizations responsible for processing EU resident's personal data must confirm that full compliance be made to ensure rights of individuals. Since cultural heritage and memory institutions are the custodian of personal data, therefore, extra care should be adopted in the process of personal data in terms of GDPR. It was also found that GDPR provides with an opportunity for these institutions to improve as well as revise various dimensions for processing the personal data and information in order to have competitive advantage. This is an opportunity which must be accepted with open arms.

In another study conducted by Hu, P., & Wei, Q. ascertain the impact of GDPR and its characteristics it has been found that GDPR has a considerable impact on personal data protection. In particular, it provides all the relevant safeguards to the compliant organizations that are needed for effective data protection. The GDPR has given individuals substantial protection right and by restricting information transaction rules for both controllers and processors. The aim is to strengthen the information area along with safeguarding the sovereignty of information between countries. Besides, it also coup up with the information technology of the modern era.

Bârsan, M. M. focused on protection of natural persons in respect of processing the data of personal nature and its free circulation. They have elaborated that the control of personal data should be with natural persons. With its various articles, the GDPR keep on strengthening the rights of data subject. The

crux of this research is to identify main rights of data subjects. The paper highlights some limitation regarding the data controllers, that adequate security should be in place to minimize the damage to data subjects. The measures include Technical and Managerial. This also ensures the data processing should be minimized. Some times the cost of security is quiet high and the user has to pay a considerable amount to data controller.

An article published by Sealey, B. analyses the achievements of new regulations and questions various ways, whereby, consumers have been affected. Other highlight of research includes improve rights of subject, enhance territorial scope, extended accountability and execution mechanisms, all of which aims to strengthen individual rights. It highlighted the emerging concerns of consumers regarding handling collection and process of storage of data. As modern technology of processing the data involves sufficient complexity therefore it would be difficult for the users to coop up with this aspect. The GDPR at one hand, shed light on complex area of law and on the other hand solidifying the role of individual control and management of the data of natural person. As digital age is throwing continuous developing challenges so the data protection legislation need to be recomposed into a system that engulfed both consent and openness. The GDPR has outweigh all previous data protection directives and regulations and provided a way, whereby, consumers enjoy more liberty in respect of personal data protection. The regulation is flexible in a to be applied uniformly into the European countries. Another important characteristic highlighted in this research is explicated that the wider scope of GDPR enable individuals raise their rights on the territory where their data is processed.

Lee, J., & Lee, E. Y. J. conducted a study in respect of personal data holder companies in Korea in the light of Personal Information Protection Act (PIPA). The research question was to ascertain effects of GDPR on the Korean based academic journals. The study reported that some important aspects pertains to GDPR were ignored in academic journals, unlike complained companies and trade organizations which retain the personal data. In addition, they also studied whether the contributors and reviewers including EU Citizens are subject to regulations of GDPR or otherwise. The research also highlighted that the aim of GDPR is to maintain sense of balance among necessity of protecting personal data with interest of important nature i.e. freedom of expression and information flow.

Basarudin, N. A., & Raji, R. A. deliberate upon points to be looked by data controller to ensure legal profiling of the personal data. The profiling process elevates innumerable issues related to personal data invasion and human privacy. The study by analyzing the international instruments and GDPR adopted the doctrinal legal method as legal resort to protect and defense activities of online data subjects. The researcher suggested to adopt design based security in profiling process owing to non-availability of system procedure to human knowledge.

Warikandwa, T. in his research study said that to address increasing cybercrimes in global financial services market that threatens the consumer's personal data. Escalating cybercrimes has made custodian of financial services to address regulations and pertinent laws for mitigating cybercrime occurrences on personal data sharing. In this connection most African countries have not yet made legislation on personal data protection. It is imperative that regulatory framework related to protection of personal data must be inherited too. This paper compared the South Africa's Protection of Personal Information Act 4 of 2013 relevancy in protecting personal data of financial services markets. The paper further discussed with the Protection of Personal Information Act clauses with GDPR guidelines.

Ievija, Ž. discussed an important issue of erasing of personal data and its anonymizing under GDPR. It is the desire of many data controllers to continue holding of personal data once its processing purpose has been accomplished. The study aimed to examine how GDPR addresses the eraser and anonymous personal data in the context of life cycle of personal data. There is an opinion that the eraser of personal data can be made if it is considered as anonymized data, however, this solution is not accepted as anonymized data can be used in big data analysis/ AI based applications.

Dumitrescu, R. M. is his study narrated that the clauses of GDPR empowers the data exporter to be both controller and processor. This creates an anomaly. GDPR allows that the transfers be implemented without prior authorization, however, the guaranties are needed via ad hoc or administrative agreement among public or supervisory authority. It is necessary that requirements were overriding the legitimate interests are fulfilled.

Usprcova, S. A study suggested that the national laws of personal data protection should be synchronized with the European legislation in order to protect state archives of Republic of Macedonia. The archives require protection from theft and illegal use. Hence, all relevant clauses of GDPR should be incorporated in order to protect archival data.

### 3. MATERIAL AND METHOD

The material was pursued through original resources i.e. the text of GDPR and CCPA along with research publications. To conduct comparison between GDPR and CCPA, a multifold strategy was adopted. All clauses of GDPR were taken into consideration in juxtaposition of CCPA were made. Moreover, a thorough literature review was conducted to identify the differences between GDPR and CCPA.

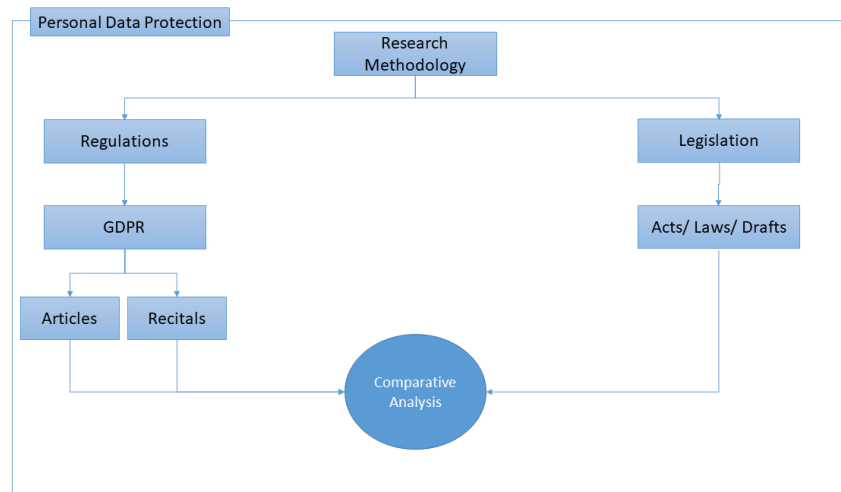


Fig 1. Reseach Methodology

In the research methodology, we first identified the broader area i.e. personal data protection. Thereafter, the regulations of data protection in the shape of GDPR were looked into. The GDPR is broadly divided into Articles and Recitals. From legislation side, the Act pertaining to consumer's privacy was perused. By juxtaposing the clauses of both sources, a comparison was made to identify the differences and this led to attaining the comparative analysis.

### 4. RESULTS AND DISCUSSION

GDPR is a legislation in the form of Regulations, enacted by European Union for protection of data. One of the important aspects of GDPR is Personal Data Protection which includes, personal information of all kinds, i.e., name, address and phone number etc. The GDPR is applicable to all European Union member States. It covers rights regarding business and citizens related data. The clauses of GDPR are very comprehensive and easy to implement.

GDPR divides in various Chapters containing certain Articles and Recitals. It is flexible in nature, i.e., every country is at liberty to adopt Clauses/Articles as per its needs. Chapter 1 contains General Provisions (Subject matter and Objectives, material and territorial scope along with definitions). Chapter 2 deals with General Principles related to Personal Data (Consents, Violations, Criminal Convictions and Offences). Chapter 3 relates to Right of Data Subjects, Transparency of information and Modalities for Exercise and Restrictions of Rights. Chapter 4 exclusively deals with Controllers and Processors of Data. Chapter 5 highlights the Transfer and Safeguards of personal data with respect to International exposure. Chapter 6 deals with Competence, Powers and Activities of Supervisory Authorities. Chapter 7 contains Dispute Resolution, Constitution of Boards, Secretariat and Confidentialities thereto. Chapter 8 provides information regards Complaint Mechanism, Judicial Remedies and Suspension of Proceedings. Chapter 9 enunciates the area of Freedom of Expression and Safeguards related to it. Chapter 10 and 11 deal with Delegation, Implementation and Final Provisions. Despite main areas every Article has sub points and few Recitals. These Recitals include examples, explanations and narrations of these Articles. There are various Articles which relates to Personal Data Protection, some of them are: Article 38 and 39 relates to right to rectification, erasure and access, portability and restrictions of data; Article 21 and 22 provides directions for marketing and profiling of data; Article 44 and 45 deals the AI and Big Data of personal data of individuals; Article 46 provides mechanism for remedies against

interference and decisions based upon them; Article 29 emphasizes four aspects of personal data, i.e., Provided data, Observed Data, Derived Data and Inferred Data.

This law was enacted through American Legislators and it is known as California Consumer Privacy Act (CCPA). It is considered the most compact and solid legislation in the domain of personal data protection. It was passed in 2018 and came into force from 1st January, 2020. The aim of enacting this law was to ensure the belief about fundamental human rights protection of citizens of California. The legislators were of the view that existing privacy should be made more secure by introducing accountability mechanism on the data holders. It includes the purpose of holding data by the companies and its onward transmission/ utilization in marketing purpose. Another striking aspect was to ensure analyzing and improving data systems.

After advent of GDPR in 2018, most of the States decided to get benefits from its clauses, however, since the GDPR was only applicable to EU countries, therefore there was a need to make legislation similar to GDPR. Thus, the California State became the pioneer of enacting California Consumer Privacy Act (CCPA). Some of the Key features of CCPA are as follows:

- Any resident or stakeholder in respect of personal data can demand from any entity responsible for collecting personal data regarding consumers;
- Any resident or stakeholder can ask for categories of information collected purpose of collection;
- Any resident or stakeholder can assume that the entity collecting the data will not gather additional categories except giving prior notice to consumer without prior notice;
- Any resident or stakeholder can demand the entity to delete his personal data which has been collected by the entity;
- Any resident or stakeholder can request the entity to apprise categories of personal data collected and sold along with information disclosed for business purposes; and
- Any resident or stakeholder can prohibit the entity to not to sell his personal data without his consent

In the area of definitions, a comprehensive definition about 'personal information' has been provided; According to that definition, personal information is the information that defines, categorizes, relates to, being related with, or could rationally be associated with a consumer or any entity. Personal information includes name, Biometric and Commercial information, account details, all kind of licenses and personal identity numbers, addresses including physical and electronic addresses, property related documents in respect of sale and purchase, web access information and location, employment and educational record, health and visual electronic and audio information and all kinds of inferences drew from customer's attitude and preferences etc

Areas of Personal Data Protection	GDPR	CCPA
<b>Scope</b>	EU Citizens, Controllers, Processors, Businesses and Data Subject even outside of EU.	All California Citizens, Business, Service Providers, Third Parties either <ul style="list-style-type: none"> <li>• Have 24 million \$ in annual revenue</li> <li>• Hold personal data of 50,000 consumers</li> <li>• Have at least half of their revenue from the sale of personal data</li> </ul>
<b>Data Type</b>	All types of personal data	Personal data that is sold for monetary or other values considerations (releasing, disclosing, transferring, or even renting of data)
<b>Basis for consent</b>	Opt in	Opt out
<b>Fines For Noncompliance</b>	Up to 20 Million euros or 4% of total global turnover from the prior fiscal year for the most severe violations. Up to 10 Million euros or 2% of total global turnover from the prior fiscal year for the less severe violations.	<ul style="list-style-type: none"> <li>• Up to \$ 7500/- No ceiling on the number of violations</li> <li>• Statutory Damages to breaches \$100 - \$750</li> </ul>
<b>Inferences and inferences drawn</b>	No specific dedicated area	Personal Information: The Statue
<b>Automated processing</b>	Mere procedural right to reverse decisions	Detailed procedural right to reverse decisions
<b>Rights of Individuals</b>	<ul style="list-style-type: none"> <li>• Right to be informed</li> <li>• Right of access</li> <li>• Right to rectification</li> <li>• Right to erasure</li> <li>• Right to restrict processing</li> <li>• Right to data portability</li> <li>• Right to object to processing</li> <li>• Rights in relation to automated decision making and profiling</li> </ul>	<ul style="list-style-type: none"> <li>• Right to request information</li> <li>• Right to data portability</li> <li>• Right to opt-out</li> <li>• Right to access data</li> <li>• Right to disclosure</li> <li>• Right to deletion</li> </ul>

Fig 2. Comparison between GDPR and CCPA highlighting the difference

From the above table it transpires that there are considerable differences between GDPR and CCPA in the context of Scope, Data Type, Basis for consent, Fines for Noncompliance, Inferences and inferences drawn, Automated processing and Rights of Individuals. However, due to comprehensiveness of GDPR it can be adopted by any State or country.

## 5. CONCLUSION

To sum up, it can be stated that GDPR is a comprehensive document which can be used for providing security of personal data. It has all the relevant clauses/ Articles that can be used accordingly. Furthermore, being dynamic in nature it has the capability to become adoptable to new changes/ technologies. However, there is a need to expand the scope of the study and conduct a comparative analysis on the basis of geographical boundaries. The future directions may include the study of laws relating to personal data protection of various developing countries in the context of the GDPR.

## REFERENCES

- Barrett, C. (2019). Are the EU GDPR and the California CCPA becoming the de facto global standards for data privacy and protection?. *Scitech Lawyer*, 15(3), 24-29.
- Veys, S., Serrano, D., Stamos, M., Herman, M., Reitingner, N., Mazurek, M. L., & Ur, B. (2021). Pursuing Usable and Useful Data Downloads Under {GDPR/CCPA} Access Rights via {Co-Design}. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* (pp. 217-242).
- Pantelic, O., Jovic, K., & Krstovic, S. (2022). Cookies Implementation Analysis and the Impact on User Privacy Regarding GDPR and CCPA Regulations. *Sustainability*, 14(9), 5015.
- Voss, W. G. (2021). The CCPA and the GDPR are not the same: why you should understand both. W. Gregory Voss, 'The CCPA and the GDPR Are Not the Same: Why You Should Understand Both,' *CPI Antitrust Chronicle*, 1(1), 7-12.
- Jordan, S., Nakatsuka, Y., Ozturk, E., Paverd, A., & Tsudik, G. (2021). Viceroy: Gdpr-/ccpa-compliant enforcement of verifiable accountless consumer requests. *arXiv preprint arXiv:2105.06942*.
- Georgiadis, G., & Poels, G. (2022). Towards a privacy impact assessment methodology to support the requirements of the general data protection regulation in a big data analytics context: A systematic literature review. *Computer Law & Security Review*, 44, 105640.
- Skendžić, A., Kovačić, B., & Tijan, E. (2018, May). General data protection regulation—Protection of personal data in an organisation. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1370-1375). IEEE.
- Grundstrom, C., Väyrynen, K., Iivari, N., & Isomursu, M. (2019, January). Making sense of the general data protection regulation—four categories of personal data access challenges. In *Proceedings of the 52nd Hawaii international conference on system sciences*.
- Papaioannou, G., & Sarakinos, I. (2018, November). The general data protection regulation (gdpr, 2016/679/ee) and the (big) personal data in cultural institutions: Thoughts on the GDPR compliance process. In *International Conference on Asian Digital Libraries* (pp. 201-204). Springer, Cham.
- Hu, P., & Wei, Q. (2020, April). Research on personal data protection of EU General Data Protection Regulation. In *IOP Conference Series: Materials Science and Engineering* (Vol. 806, No. 1, p. 012003). IOP Publishing.
- Bârsan, M. M. (2018). A Partial Overview of the Data Subjects' Control over Their Personal Data under the General Data Protection Regulation. *Bulletin of the Transilvania University of Braşov, Series VII: Social Sciences and Law*, 11(2), 129-134.
- Sealey, B. (2020). Has the 2016 General Data Protection Regulation really given consumers more control over their personal data?. *LJMU Student Law Journal*, 1, 17-41.
- Lee, J., & Lee, E. Y. J. (2019). Personal data protection of academic journals in the age of the European General Data Protection Regulation: guidelines for Korean journals. *Science Editing*.
- Basarudin, N. A., & Raji, R. A. (2022). Implication of Personalized Advertising on Personal Data: A Legal Analysis of the EU General Data Protection Regulation. *Environment-Behaviour Proceedings Journal*, 7(22), 109-114.
- Warikandwa, T. (2021). Personal Data Security in South Africa's Financial Services Market: The Protection of Personal Information Act 4 of 2013 and the European Union General Data Protection Regulation Compared. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 24(1).
- Ivriņa, Ž. (2022). Erasure and Anonymisation of Personal Data in Context of General Data Protection Regulation.
- Giménez, A. O. (2021). The impact of the general data protection regulation of the european union on the legal regime of international transfers of personal data. *Spanish Journal of Legislative Studies*, (3), 1-16.
- Dumitrescu, R. M. (2018). Processing of personal and medical data by judicial institutions in the context of the enforcement of Regulation EU 2016/679-General Data Protection Regulation (GDPR). *Journal of Comparative Research in Anthropology & Sociology*, 9(1).

---

Usprcova, S. (2018). The State Archives of the Republic of Macedonia: Use of Archival Material and Data Protection Pursuant to the Law on Personal Data Protection and the General Data Protection Regulation. *Atlanti*, 28(2), 91-98