International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

# Tracing the Impact of GDPR on Global Data Privacy

**Khushal Chauhan[1], Mayur Ghawate[2], Saachi Joshi[3], Shrikant Kawade[4]**

[1]Vishwakarma University, Department of Science and Technology, Kondhwa, Pune- 411048, India
Email: *khushal0519[at]gmail.com*

[2]Vishwakarma University, Department of Science and Technology, Kondhwa, Pune- 411048, India
Corresponding Author Email: *mayurghawate17[at]gmail.com*

[3]Vishwakarma University, Department of Science and Technology, Kondhwa, Pune- 411048, India
Email: *saachi.joshi26903[at]gmail.com*

[4]Vishwakarma University, Department of Science and Technology, Kondhwa, Pune- 411048, India
Email: *shrikantsk1224[at]gmail.com*

**Abstract:** ***The General Data Protection Regulation GDPR, enacted in May 2018, has reshaped data protection standards globally, enforcing strict requirements on organizations to protect personal data. This paper evaluates the impact of GDPR on modern cybersecurity practices, analyzing its influence on organizational policies, case studies of major breaches, cost benefit analyses, and geopolitical comparisons of data protection laws. The research highlights significant shifts in data privacy strategies and presents best practices for compliance, offering recommendations for future regulatory adaptations.***

**Keywords:** GDPR, cybersecurity, data privacy, information security, data protection

## 1. Introduction

Implementing data protection laws across various countries has become a critical aspect in this digital world. Various countries have implemented their own data protection law like California Consumer Privacy Act (CCPA), and Health Insurance Portability and Accountability Act (HIPAA) in USA. Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada and Personal Data Protection Bill (PDPB) in India. Similar to these countries Europe has also implemented its own data protection law which is General Data Protection Regulation (GDPR). The significance of GDPR cannot be ignored. GDPR sets a high standard for data protection, influencing not only European organizations but also those outside Europe handling European citizens confidential information.

This law has enforced many organizations to re-evaluate their security practices and implement strong security measures, ensuring transparency in their data handling practices. GDPR's impressive scope has significantly influenced many countries in implementing data protection and privacy laws. After GDPR came into the effect it included various provisions where companies incurred high penalties for non-compliance of pro-visions where they failed to protect the consumers data. Thereby raising the global standards for data protection and privacy.

## 2. Objectives of the Research

The following are the objectives of our research Paper:

- To analyse the changes in security policies and practices before and after the implementation of GDPR.
- To investigate the impact of GDPR law on the overall cybersecurity culture within organizations.
- To present case studies of the organizations that have faced data breaches.
- To examine the cost-benefit analysis of GDPR compliance.
- To compare GDPR with other countries data protection and privacy laws and understand its impact.

## 3. Literature Review

In a previous study by Dragan Savić, Mladen Đuro Veinović in year 2018, it was observed that companies maintaining the data on EU citizens must make sure that they follow GDPR policies to avoid heavy fines. The research mainly focused on the importance of following proper approach to GDPR compliance and their policies. The analysis pointed out that GDPR plays an important role in the documentation that data controllers must take accountability of user's confidential data. Moreover, the study highlighted the new antitrust-type sanction under GDPR. Emphasizing the seriousness of the data protection and privacy they enforced penalties of up to 4% of annual worldwide income or €20 million. Eventually, while the consequences of disobeying the law are serious, companies following GDPR laws have seen positive results in protecting data.[1]

According to the research conducted by Rossana Ducato July 2020, Under GDPR they analyzed the legal structure for processing personal data in scientific research. Regardless of GDPR's intention to synchronize data protection acts across the Europe, member states have the rights to get involved with specific provisions for scientific re-search. The study also showcased those various provisions, such as Articles 13 and 14, have certain flaws with respect to content. Moreover, the study also pointed that there is lack of quality of including small details in GDPR's provisions.[2]

An analysis conducted by Livia Puljak, Anamarija Mladinić, Ron Iphofen, and Zvonimir Koporc in year 2020. This research cited that The Croatian Person-al Data Protection Agency (CPDPA) experienced changes in data protection inquiries from January 2015 to the end of 2019, especially after the introduction of GDPR. Pre-GDPR duration, It reported 21 requests about research data protection, and 16 similar requests were found in post-GDPR. In 2018, the number of requests and complaints hiked, it was reported that there were 356 complaints about data protection violations and 3,464 requests for legal advice. The major issues reported were employee data handling, video surveillance, and excessive personal data disclosure. This highlighted GDPR's effect on increasing awareness and requirements in data protection practices.[3]

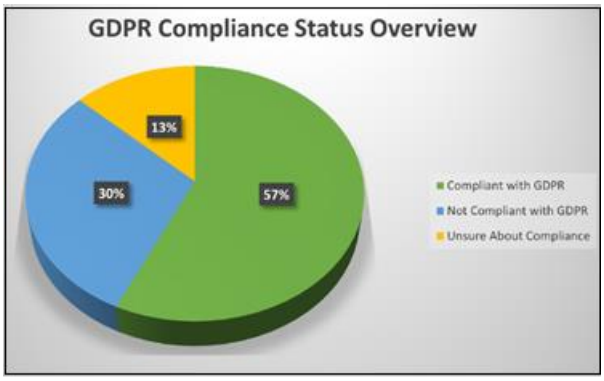


**Figure 1**

According to research conducted by the European Business Awards on behalf of RSM, they found out the following results about the European business [18]:
Compliant with GDPR: 57%
Not Compliant with GDPR: 30%
Unsure About Compliance: 13%

## 4. Case study

British Airways GDPR Fine
The United kingdom's Airline - British Airways (BA) experienced a critical data breach in September 2018, where hackers diverted user traffic from the original British Airways website to a duplicate and fraudulent site. This caused leak of personal information stored on the website, around 400,000 users' data were com-promised. The ICO, the UK's (Information Commissioner's Office) during the investigation they found that BA had violated Articles 5(1)(f) and 32 of the General Data Protection Regulation (GDPR), the investigation found out that their website did not follow proper security measures. The ICO initially proposed to fine the Airways €204.6 million (£183.39 million). Although, this penalty was later reduced to $26 million due to COVID-19 pandemic. The officers mentioned that this fine was not only due to the data breach but mostly because the airline did not follow proper security protection mechanisms. This case study highlights the critical importance of implementing strong security measures to safeguard the customers information or if they failed to follow GDPR'S guidelines they may face hefty penalties. It also highlights the ICO's commitment to enforcing data protection laws and the significant impact of regulatory actions on business practices.[4] [5]

**Case Study: Meta's GDPR Fine**
In May 2023, the Irish Data Protection Commission (DPC) imposed a huge penal-ty on Meta €1.2 billion for not compiling with the Europe's General Data Protection Regulation (GDPR). Meta was found transferring personal data of European users to the U.S. without robust protection. The Irish commission instructed Meta to suspend future data transfers and start complying with GDPR's policies within six months. Meta, the parent company of Facebook, Instagram, and WhatsApp, was found guilty in violating of GDPR Articles 5(1)(f) and 32. The fine imposed Meta to discontinue transferring personal data to the U.S. within five months and to stop illegal data processing and storage. Despite this Meta has been frequently found violating the regulations of GDPR in January and they were fined €390 mil-lion for forcing users to accept ads for using Facebook. Moreover, in November they were again fined €265 million for data leak. Meta's significant fine emphasizes the critical importance of data protection measures and the impacts caused by non-compliance of GDPR. This case study was an awakening call for many multinational companies handling European citizens data, focusing for the need of robust and secured data transfer and protection mechanisms.[6] [7]

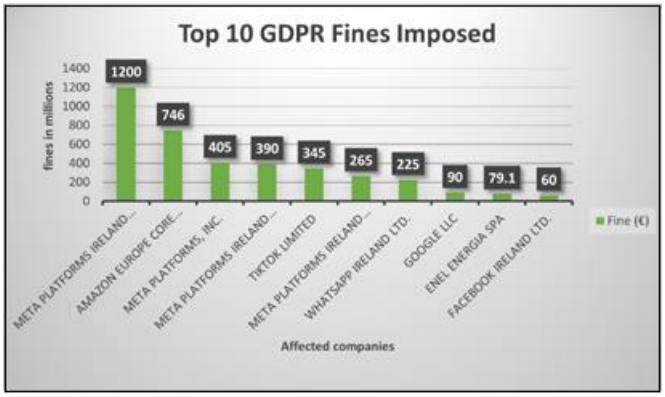


**Figure 2**

The above Graph demonstrates about the Top 10 fines imposed by GDPR (in millions) with me-ta platform being highest with €1200 million and Amazon with €746 million.
These stats and figures are being given by Enforcement Tracker (enforcementtracker.com) [17]

## 5. GDPR Provisions and their Associated Fines

**Table 1**

| Articles | Description | Fines for non-compliance |
|---|---|---|
| Article 5 | Principles of Data Processing: This article establishes core principles for personal data which shall include lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, and integrity/confidentiality | Up to €20 million or 4% of annual global revenue, whichever is higher. |
| Article 6 | Lawfulness of Processing: This article summarizes the situations of the user's data processing is lawful, including consent, contractual necessity, legal obligation, vital interests, public task, and legitimate interests. | Up to €20 million or 4% of annual global revenue. |
| Article | Security of Processing: This article | |

| | | |
|---|---|---|
| 32 | requires companies to implement appropriate relevant technical and organizational measures to ensure security of data, such as encryption of personal data and confidentiality, integrity, availability. | Up to €10 million or 2% of annual global revenue, whichever is higher. |
| Article 45 | Transfers on the Basis of an Adequacy Decision: In this article it mentions about the transfer of per-sonal data to countries outside the EU that provide an adequate level of data protection. | Up to €20 million or 4% of annual global revenue. |
| Article 83 | General Conditions for Imposing Administrative Fines: Describes a group of approach of fines based on the severity and nature of the GDPR violation. Minor violation may suffer lower fines, while severe breaches, particularly those related to core principles like consent and data subject rights, can result in the highest fines. | Minor breaches: Up to €10 million or 2% of global revenue. Severe breaches: Up to €20 million or 4% of global revenue. |

This table provides a Brief summary of the important GDPR provisions and their associated fines. This highlights the notable financial risks that companies may face due to event of non-compliance of policies. It also underlines the importance of complying GDPR requirements to avoid heavy penalties which can have a serious financial impact on the organization. [8] [9] [10] [11]

## 6. Implementation Timeline and Milestones:

On April 14, 2016 the General Data Protection Regulation (GDPR) was officially adopted by the Parliament of Europe and the Council of the European Union. This was marked as a significant evolution of data protection laws across the Europe, this was designed to implement data protection and privacy laws. This was brought in to protect all European citizens personal data privacy, and reshape the way organizations use user's data more securely. The GDPR became enforceable on May 25, 2018. During the period of 2016 to 2018 the organizations were given time span of two years to adjust policies, procedures and systems to ensure with the new GDPR compliance requirements. Unlike previous policies, GDPR is a new regulation, which means it will be applicable to all the countries in Europe. Introduction of GDPR replaced the 1995 Data Protection Directive (DPD). The major Key points of GDPR included the introduction of Data Protection Impact Assessments (DPIAs) to identify and reduce risks in data processing. This also included the appointment of Data Protection Officers (DPOs) which were necessary to make sure that companies follow compliance.[12] [13]

## 7. Impact on cybersecurity culture

The commencement of GDPR had a profound influence on corporate culture, significantly boosting the need for data protection. The introduction of this policy has obligated all organizations to take data protection and privacy regulations severely. This led to a change in culture in the organization in handling users' data with topmost confidentiality. Embedding GDPR principles, the organizations have become more active in securing data. This change in regulation has also seen increase in employee training and awareness regarding data protection. Which has led to training of employees at regular intervals with the updated knowledge regarding latest trends and best security practices that should be followed in corporate sector. These training and awareness program should be mandatory to those employees who deals with handling personal data and are well versed with GDPR requirements. The priorities of administrator have changed significantly after the implementation of GDPR. This has led management for the creation of new roles or positions such as Data Protection Officers (DPOs). These officers play an important role in ensuring that their companies and employee's handles the personal data of supplier's customers and other individual with respect to data protection regulation. According to the (Regulation (EU) 2018/1725) the Union institutions, bodies, offices and agencies are required to appoint DPO. Similarly, Regulation (EU) 2016/679, which obliges to some organizations within Europe member states, for the appointment of a DPO. Companies have heavily invested in updating their enhancing cybersecurity measures, protection infrastructures, and ensuring robust data handling practices. This change has influenced specific budget allocations which we will be discussing further.[12] [13]

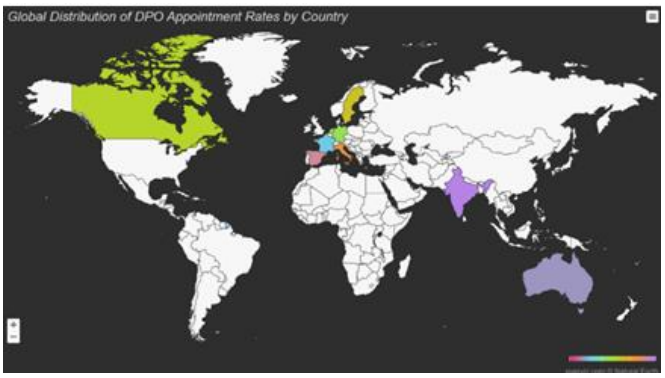


**Figure 3**

The above map highlights the "DPO Appointment Rates Across Selected Countries"- a survey conducted by Deloitte.[20]

## 8. Cost analysis of GDPR Compliance

Many companies have faced significant financial implications while assuring to comply with the General Data Protection Regulation (GDPR). These costs may include various factors like hiring the Data Protection Officers (DPO) for the companies, investing in the latest technology used for data protection, conducting staff and employee training, regularly con-ducting security awareness programs and more overly changing existing systems with up-dated infrastructural systems. Further, the organization should also keep in mind about the cost related to legal consultations, external security audits, and potential penalties for non-compliance of the law. Following GDPR measures it involves several costs which can be direct and indirect. The Direct costs may include upgrading IT infrastructure, cybersecurity measures, and the upskilling of the skills of staff and employees to handle GDPR-specific roles. Indirect costs may include disruptions during the implementation phase, such as downtime during system updates. Despite the financial burden, implementing GDPR compliance offers various benefits. The company may gain customers trust,

showing organizations commitment and transparency in protecting their data and privacy, which is the very important aspect to survive in the competitive market. Organizations could also experience a less data breach, which may lead to cost savings due to breach response, legal liabilities, and reputation damage. Complying to GDPR could help organizations to avoid hefty fines and penalties that can arise from policy violations. A good reputation against data protection may increase the investors' confidence, which may also lead to increase in organizations valuation.

## 9. Geopolitical Comparisons in Data Protection Regulations

1) General Data Protection Regulation (GDPR) - European Union

**Scope:** GDPR is applicable to all organizations, regardless of where the organization is located. The main focus is based on protecting personal data of the users located in Europe. GDPR has set high standards globally for data protection.

**Key Features:**

- For data processing it requires exclusive permission from users.
- This law provides rights to users, such as right to delete, access, and modify their own data.
- Non-compliance of GDPR, will impose significant penalties up to 4% of global annual turnover or €20 million, whichever is higher.
- It is also Mandatory for the organizations report any kind of data breaches to the relevant authorities within 72 hours and they should also inform the users whose data has been leaked.

2) California Consumer Privacy Act (CCPA) - USA

**Scope:** CCPA applies to businesses that operate in California and any for-profit organisation which collects the data of the users. And fulfils any one of these criteria: -

a) Has annual income above $25 million.
b) Contains personal information of 50,000 or more users or devices.
c) 50% or more annual income from selling personal data.

**Key Features:**

- This law allows users the right to know that how personal data is being disclosed, sold and collected without the consent.
- This also Provides the user the right to delete their data when requested.
- Compared to GDPR the penalties in this law are less sever but if violated could lead to laws suite and damages.
- The fine is Up to $2,500 or more per violation for Unintentional Violations and Up to $7,500 per violation for Intentional.

3) Personal Information Protection and Electronic Documents Act (PIPEDA) - Canada

**Scope:** This law governs the collection, usage, or disclosure of personal information. PIPEDA (Personal Information Protection and Electronic Documents Act) is applicable to organizations across Canada, that handle the personal information of company's users.

**Key Features:**

- This law Requires organizations to get permission from the user before collecting their personal information like Credit records, loan records, name, age, ID number, and employment details.
- This also Provides right to every induvial to access and correct their information which is held by the organization.
- It also highlights the transparency of how personal data is handled by the organization, PIPEDA can fine up to CAD $100,000 per violation.
- Personal Information Protection and Electronic Documents Act (PIPEDA) is En-forced by OPC (Office of the Privacy Commissioner of Canada), with a aim of im-posing policy rather than implementing penalties.

4) INDIA's: Digital Personal Data Protection Bill (DPDP) – 2022 and Personal Data Protection Bill (PDPB) - 2019:

**Scope:** The similar version of Personal Data Protection Bill was the Digital Personal Data Protection Bill which was the simplified version of 2019's PDPB. This bill will be applicable in India where users' personal data is collected, it will also be applicable to the organization outside of India if they are offering any goods or services in India.

**Key Features:**

- The DPDP make sure that data must be used with the consent of the user. This consent must be freely given, specific, and explicit.
- All users have the right to withdraw their consent of sharing their information at any time
- Users can request for the transfer from one service provider to another of their personal data.
- DPDP also allows for cross-border transfers of personal data to some trusted countries or regions.
- There are certain fines for non-compliance of DPDP which can go up to ₹250 crore ($30 million USD) per violation. If an organization fails to notify the authorities for the data breach, they can face penalties of up to ₹200 crore ($24 million USD).[14] [15] [16]

## 10. Significance

This study is significant because it evaluates how the GDPR has transformed global data protection practices, setting new standards for organizations worldwide. By examining case studies and legal frameworks, the research underscores the laws global impact on cybersecurity policies.

## 11. Conclusion

This study illustrates how the GDPR has reshaped data protection standards and influenced organizational behavior globally. Through case studies and cost analyses, the research highlights the importance of strong data privacy practices and compliance. As cybersecurity threats evolve, GDPRs framework will continue to play a crucial role in shaping global privacy laws, offering key insights for future regulatory frameworks. As data protection laws will continue to evolve globally, the lessons learned from GDPR will remain vital in shaping the future of cybersecurity and privacy laws.

## References

[1] [1] D. Savić and M. Veinović, "Challenges of General Data Protection Regulation (GDPR)," in Sinteza 2018 - International Scientific Conference on Information Technology and Data Related Research, Belgrade, Singidunum University, Serbia, 2018, pp. 23-30. doi: 10.15308/Sinteza-2018-23-30. Available: https://doi.org/10.15308/Sinteza-2018-23-30
[2] R. Ducato, "Data protection, scientific research, and the role of information," Computer Law & Security Review, vol. 37, 2020, Art. no. 105412. https://doi.org/10.1016/j.clsr.2020.105412
[3] L. Puljak, A. Mladinić, R. Iphofen, and Z. Koporc, Biochem Med (Zagreb), vol. 30, no. 3, Art. no. 030201, Oct. 2020. doi: https://doi.org/10.11613%2FBM.2020.030201
[4] "British Airways: A Case Study in GDPR Compliance Failure." SourceDefense. Available: https://sourcedefense.com/resources/blog/british-airways-a-case-study-in-gdpr-compliance-failure/ Accessed: Aug. 6, 2024.
[5] "ICO Reduces British Airways GDPR Fine to £20 Million for 2018 Data Breach." Data Privacy Manager. Available: https://dataprivacymanager.net/ico-reduces-british-airways-gdpr-fine-to-20-million-for-2018-data-breach/ Accessed: Aug. 6, 2024.
[6] "Meta Hit with Record €1.2B GDPR Fine." Data Privacy Manager. Available: https://dataprivacymanager.net/meta-hit-with-record-e1-2b-gdpr-fine/ Accessed: Aug. 6, 2024.
[7] C. C. Miller, "Meta Hit with Record $1.2 Billion Privacy Fine by EU," The New York Times, May 22, 2023. Available: https://www.nytimes.com/2023/05/22/business/meta-facebook-eu-privacy-fine.html Accessed: Aug. 6, 2024.
[8] "Article 5 GDPR: Principles Relating to Processing of Personal Data." GDPR-Info. Available: https://gdpr-info.eu/art-5-gdpr/ Accessed: Aug. 9, 2024.
[9] "Article 6 GDPR: Lawfulness of Processing." GDPR-Info. Available: https://gdpr-info.eu/art-6-gdpr/ Accessed: Aug. 9, 2024.
[10] "Article 32 GDPR: Security of Processing." GDPR-Info. Available: https://gdpr-info.eu/art-32-gdpr/ Accessed: Aug. 9, 2024.
[11] "Article 45 GDPR: Transfers on the Basis of an Adequacy Decision." GDPR-Info. Available: https://gdpr-info.eu/art-45-gdpr/ Accessed: Aug. 9, 2024.
[12] "Data Protection Officer (DPO)." European Data Protection Supervisor. Available: https://www.edps.europa.eu/data-protection/data-protection/reference-library/data-protection-officer-dpo_en#:~:text=The%20primary%20role%20of%20the,the%20applicable%20data%20protection%20rules Accessed: Aug. 12, 2024.
[13] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the Protection of Individuals with Regard to the Processing of Personal Data by the Union Institutions, Bodies, Offices, and Agencies. EUR-Lex. Available: https://eur-lex.europa.eu/eli/reg/2018/1725/oj Accessed: Aug. 12, 2024.
[14] "CCPA Compliance Checklist." Securiti. Available: https://securiti.ai/blog/ccpa-compliance-checklist/ Accessed: Aug. 12, 2024.
[15] "PIPEDA." Delphix. Available: https://www.delphix.com/glossary/pipeda Accessed: Aug. 12, 2024.
[16] Ministry of Electronics and Information Technology, Government of India, Digital Personal Data Protection Act, 2023. Available: https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf Accessed: Aug. 12, 2024.
[17] "Insights." Enforcement Tracker. Available: https://www.enforcementtracker.com/?insights Accessed: Aug. 12, 2024.
[18] "30% of European Businesses Are Still Not Compliant with GDPR." RSM. Available: https://www.rsm.global/insights/data-privacy-and-cyber-security/30-european-businesses-are-still-not-compliant-gdpr#:~:text=21%25%20of%20businesses%20admitting%20that%20they%20still%20have%20no%20cyber%20security%20strategy%20in%20place Accessed: Aug. 12, 2024.
[19] "GDPR Statistics." Forms.app. Available: https://forms.app/en/blog/gdpr-statistics Accessed: Aug. 12, 2024.
[20] GDPR Six Months On. Deloitte, 2018. Available: https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/risk/deloitte-uk-risk-gdpr-six-months-on.pdf Accessed: Aug. 12, 2024.

## Author Profile

**Khushal Chauhan** is a Student at Vishwakarma University, Kondhwa, Pune-411048, Indiawho is currently (2024) studying BTech Computer Engineering (Cyber Security Specialization)

**Mayur Ghawate** is a Student at Vishwakarma University, Kondhwa, Pune-411048, Indiawho is currently (2024) studying BTech Computer Engineering (Cyber Security Specialization)

**Saachi Joshi** is a Student at Vishwakarma University, Kondhwa, Pune-411048, India who is currently (2024) studying BTech Computer Engineering (Cyber Security Specialization)

**Shrikant Kawade** is a Student at Vishwakarma University, Kondhwa, Pune-411048, Indiawho is currently (2024) studying BTech Computer Engineering (Cyber Security Specialization)