RETROSPECTIVE ANALYSIS ON THE IMPACT OF INTRODUCING GDPR AND DPDPA ON EXISTING COMPANIES, SME'S AND START-UPS

Jayaram Iyer, School of Law, RV University

ABSTRACT

Data privacy is a relatively newer adaptation that has proven to be of merit due to its compliance standards and importance specified on safeguarding the critical information of every individual whose data is utilized. This paper provides for a review of the impact that the General Data Protection Regulation (GDPR) in the European Union and the Digital Personal Data Protection Act (DPDPA) in India have had on businesses across different stages of development. It examines the compliance challenges, changes made to resume operations, and strategic changes made by existing companies, small and medium-sized enterprises (SMEs), and emerging start-ups. Through highlights of the financial, technological, and administrative implications of these data protection regimes, this paper also explores how these laws have influenced innovation, growth, consumer trust, and cross-border data flows. The insight of this paper also explains the differed degrees of preparedness, resilience, and agility among businesses, which allows the policymakers and entrepreneurs into furthering the scope of these statutory provisions and enables smoother transitions in navigating the evolving data protection landscape.

INTRODUCTION

The inception of the Data protection Directive[1] was a valiant step towards respecting the legal security of individuals against misuse of information relating to them. The EU has always pioneered in recognising human rights to reign supreme and the DPD was an exemplary display for the same. But the DPD was, however, more about the rights and interests of individuals and not mainly pertaining to the "DATA" of those individuals, as the name might suggest. Regardless, this was a preliminary step to enhancing the recognition of Privacy laws in the EU. There were tangible challenges associated with execution of DPD across the EU, primarily because its application was limited by the national regime of the member states. But the DPD served as a notable reminder to all the companies indulging in trade practices to not be entirely market focused and to be flexible enough to comply with privacy regulations into their business models. Eventually, the DPD was replaced by the General Data Protection Regulation in 2018 to modernize and strengthen the pre-existing data protection laws. But this introduction of the GDPR introduced a plethora of challenges to companies. The GDPR is a comprehensive legal framework that prioritizes the protection of personal data for the European Union. Its core principles revolve around transparency, accountability, and allows control over the data to the individuals. The GDPR has stringent requirements for data collection, processing, storage, and transfer, applying not only to EU-based companies but also to foreign businesses offering goods or services within the EU jurisdiction. India's DPDP Act of 2023, takes inspiration from the GDPR and reflects a similar approach to safeguard personal data. The act focuses on transparency, consenting data processing, and ensuring that businesses adopt robust data security measures. However, the DPDP Act takes a graded approach to compliance, offering leniencies for smaller businesses and start-ups.

IMPACT ON EXISTING CORPORATIONS

Large, established corporations have the resources and infrastructure to adopt the operational and financial costs of compliance with regulations like GDPR and DPDP Act. But, the transition is seldom seamless, as it requires restructuring and further investments into newer technologies.

[1] Directive 95/46/EC of the European Parliament and of the Council., *Official Journal L 281 ,P. 0031 – 0050*, Document 31995L0046, 24 Oct 1995.

In terms of operational regulations, large corporations have had to overhaul their systems to keep up with the guidelines issued by the data protection authorities. Companies like Meta and Google had to invest heavily into reworking their privacy policies and ensuring consent for the usage of the data and providing adequate transparency regarding the entire transaction. Meta has undergone severe penalties for lack of compliance with the GDPR on multiple occasions, which shows the seriousness behind enforcement of privacy in the EU. Their efforts to realize the importance of Privacy has been recognized as a global standard for data protection and India through the DPDP Act also hopes to achieve the same levels of privacy laws.

The major hurdle of compliance with such laws for existing companies is the sheer financial burden that has to be undertaken by them, additional upgrades to their infrastructure and hiring of data protection officers in the case of GDPR compliance and providing regular audits as per the DPDP Act. But there is a silver lining that arises out of this, strict compliance with the GDPR and DPDP Act, whichever applicable, allows for a strong customer feedback and confidence in the company's actions, while also ensuring that there would be a significantly reduced risk of legal actions upon the company. Microsoft swiftly gained recognition for having such a proactive approach to data protection and adapted easily to the introduction of the GDPR because they were already having such norms to being privacy conscious, which allowed them to gain a competitive advantage in the EU, where even before the GDPR was enforced, microsoft would ensure that they had in-house laws based on the DPD, such as EULA to ensure that the consumer of the brand had a clear picture of what their role was in the entire exchange of the company.

The strict adherence to the GDPR and DPDP Act was a chance for some companies to pivot into a different business model. Because privacy was a non-negotiable element because of GDPR and DPDP Act, these companies opted for a privacy-by-design principle and companies like Apple and Rockstar Games turned data protection compliance into a marketing tool and made it their unique selling point to further highlight their commitment to their users.

IMPACT ON SMALL AND MEDIUM ENTERPRISE (SMEs)

The lack of resources and limited expertise creates a negative atmosphere for SMEs to adapt to data protection regulations. For such companies, sudden enforcement of privacy laws can do more bad than good, because failure to adopt such laws degrades them of their credibility,

but any effort made towards adopting these regulations would impose excessive financial and operational burdens that may even result in closure or bankruptcy of the company. SMEs often lack the financial and operational resources needed for compliance. Under the GDPR, there are minimal pardons for SMEs and every business must ensure that they maintain appropriate records of processing data, which is a herculean task for a small business without dedicated personnel. The expectation of the GDPR and DPDP Act in terms of companies introducing encryptions, anonymization and breach management systems are unrealistic when considering such small businesses. A 2020 survey by the European Commission found that 75% of SMEs in the EU faced difficulties in implementing GDPR compliance measures. The costs of legal consultations, IT upgrades, and awareness training were cited as major hurdles. However, SMEs that successfully adapted showed improved customer trust and competitive positioning.

IMPACT ON START-UPS / NEW BUSINESSES

startups and newer businesses that have been set up after the provisions of GDPR and DPDPA, have a relatively easier time in ensuring data protection mechanisms are adhered to, mostly because they have the opportunity to integrate these mechanisms as part of their company and embed these norms from the very foundation. The key feature of such new companies is their business strategies and the innovation that allows for their introduction into the existing market. If such companies have a competitive edge over the existing companies and if they can also introduce it with pre-provisioned sanctions for data protection, then that automatically provides for credibility and recognition. But they too have certain issues in applying the rules of GDPR and DPDP Act.

Perhaps the greatest challenge of a start up in trying to adapt Data Protection laws is the fact that the cost of compliance would inevitably divert their limited resources from their core business associated expenses. And if it happens to be a bootstrapped start-up, then they'd be forced to raise capital out of desperation, which can have further adverse effects on the growth of the company. If the company happens to be a product-based company or a software-based start-up, then they would face undue delay in market entry, purely because of the need for compliance certifications. Another drawback would be the limited flexibility that the start-ups have towards utilizing the data that was collected. Prior to the introduction of the GDPR and DPDP Act, there were limited restrictions in terms of using the customer's information for

marketing purposes and further market reach, this allowed a lot of companies to capitalize on this, allowing them to be successful, but unfortunately, the current start-up companies do not have that opportunity.

DuckDuckGo, a search engine start-up used the GDPR compliance measures to reintroduce themselves to be privacy-centric and used this to carve out a niche in the global market for themselves. This garnered them a lot of attention, which they further capitalized by announcing the $500,000 DuckDuckGo privacy challenge in 2018, which resulted in the Tor Project, an anonymity- network based NGO that specializes in privacy and data protection to come into a partnership with DuckDuckGo for their state-of-the-art privacy models in search engines[2].

The grading system introduced by the DPDP Act does offer start-ups with ample flexibility for start-ups and newer businesses, therefore reducing the compliance burden. For example, any start-up which has limited data-processing activities as part of their business do not have to appoint a Data Protection Officer, allowing them to focus on their original goals.

SECTOR-SPECIFIC IMPACT OF GDPR AND DPDP ACT

1. E-commerce, Quick commerce and Retail commerce:-

Data protection laws have significantly impacted the traditional and newer variations of this market space, where consumer data is the driving force behind the success of this sector. The manipulation of user data for personalized marketing and sales strategies was rampant since the turn of the century until the implementation of the GDPR, and later the DPDP act. The introduction of these laws ensured explicit consent seeking from the individuals whose data was assimilated. This forced Amazon to redesign their cookie policies and opt-in mechanisms. Similarly, in India, Flipkart had to adhere to the norms of DPDP Act and adopt such a change, while ensuring increased transparency in data collection and usage. Another such trend was the sudden boom in investment in India seen in secure payment gateways and fraud detection systems[3] as

[2]The Tor Project Joined the $500,000 DuckDuckGo Privacy Challenge 2018 https://blog.torproject.org/tor-project-joined-duckduckgo-privacy-challenge-2018/, March 13, 2018, last accessed on January 26, 2025.
[3] Zehra F and others, "Exploring Consumer Preferences and Behaviour toward Digital Payment Gateways in India" (2024) 41 International Journal of Experimental Research and Review 158, https://doi.org/10.52756/ijerr.2024.v41spl.013

a tool to win over customers' trust.

2. **Healthcare Systems:-**

The implementation of the GDPR and DPDP Act was a major boon to the healthcare sector, purely because of the sensitive nature of the data that was collected through these sources and the sheer quantity of data that was taken could have been misused, affecting a large segment of society at large. The Dutch Haga Hospital was the first healthcare body to receive a GDPR fine for non-compliance[4]. This level of attention towards data security is yet to be observed in the Indian context vis-à-vis the DPDP Act, as currently, the Indian healthcare systems are not adapting to data compliance as there isn't strict regulation for the same. It should be mandated to invest in electronic medical record systems and encryption technologies. Telemedicine platforms are seeing a rise in India, with the application of online platforms like Practo and 1mg, but currently, there are no adequate measures to ensure compliance with DPDP for the sake of patient confidentiality.

3. **Technology and Software-as-a-service (SaaS) fields:-**

Compliance was easily accepted by tech and SaaS Companies, purely because of the virtual nature of the work, allowing for immediate adaptation of GDPR and DPDP Act frameworks to establish data security. Indian and Western SaaS companies are positioning themselves as data protection compliant solution providers and consultation services to ensure that they can mediate and assist with further implementation of the privacy laws. Salesforce Inc is a clear example of using GDPR compliance as a value proposition to differentiate themselves from the global market.

4. **Financial Management and Fin-tech domains:-**

Because of the strong regulatory bodies that exist globally to safeguard any and all monetary transactions, the implementation of GDPR and DPDP Act regulations was swift and of minimal efforts, therefore allowing banks and financial institutions to

[4] Ilias Abassi and Richard van Schaik, DLA Piper, The Netherlands - *First GDPR fine imposed: EUR 460,000, Lexology,* July 16, 2019. https://www.lexology.com/library/detail.aspx?g=f85b5cfe-b645-4956-a954-fa54b12eb857, Last Accessed on January 26, 2025, 1800 Hrs.

strengthen their cybersecurity measures. This mandated protection of customer data during their entire transaction within the realm, to ensure accountability for any misappropriation of funds and tracking of payments. European banks have implemented two-factored authentication systems to comply with GDPR's requirements. In India, the Reserve Bank of India has incorporated DPDP Act guidelines into its data security policies, enabling financial institutions to enhance their data governance frameworks.

5. **Ed-tech and training programs:-**

The educational sector was not the direct aim of introducing privacy regulations like GDPR and DPDP Act, but there were segments that were capable of being compliant-ready, specifically those institutions that offered online courses and training models. This also speaks of the cross-territorial nature of GDPR, as a portion of the affected students were from different countries, predominantly from Asia. Many universities In the EU had to adapt and redo their admission process and the alumni and student communication processes. The GDPR provided the platform to protect student data and obtaining explicit consent for its usage[5]. In India, the DPDP Act directed Ed-tech platforms like PhysicsWallah and Unacademy to implement similar measures under DPDP Act, ensuring that user data is handled responsibly.

COMPARATIVE ANALYSIS OF GDPR AND DPDP ACT

The foundation of the DPDP Act was established by the implementation of the GDPR in the EU, which acts as a beacon of hope for privacy laws across the world. Although the foundational idea behind both the laws remains the same, the method of application differs in certain aspects such as, the scope and applicability, where GDPR is applicable to the EU and any foreign entity that is participating in handling the data of EU individuals, whereas the DPDP Act is applicable towards the businesses operating in India. Despite the foundation for data protection being set by GDPR, India's DPDP Act is more lenient towards SMEs and start-ups, therefore allowing the business to establish themselves before they apply stringent rules

[5] Tattersfield, Kate, How universities have to adapt under the new EU General Data Protection Regulation (GDPR), January 7, 2025, < https://www.fullfabric.com/articles/how-universities-have-to-adapt-under-the-new-eu-general-data-protection-regulation-gdpr#:~:text=GDPR%20will%20be%20applicable%20to,data%20processing%20affects%20EU%20citizens)., last accessed on January 26, 2025, 1800 Hrs

and regulations against them, which is not the case with GDPR, where the law applies the same to all businesses, irrespective of the size and quality. And likewise, the GDPR imposes much stricter penalties, which can go upto 20 million Euros, or 4% of the company's global turnover, whichever is higher., whereas in India, the violation is not as strongly penalized, instead the DPDP Act provides for a graded approach, which varies the penalties from 10,000 Rupees to 2,500,000,000 Rupees, while considering multiple reasonings such as the gravity of the violation, the structure of the company, the age of the company et cetera., and instead allows for education the offence and provides for correction and allows for growth of SMEs and start-ups.

GOAL OF GDPR AND DPDP ACT

The prominent goal of the evolution from DPD to GDPR and recently, the development of the DPDP Act, is to ensure a global standard of application of data protection laws. The evolution of privacy laws shows the shift in the global paradigm in their approach towards addressing data protection and management. It is stronger than ever before, and it is only now considered with more weightage. But this does not signify the end, if anything this is merely the initial stages of data protection. In the course of time, these regulations aim towards ensuring consumer safety and gaining their trust, allowing for consumer confidence to grow based on the actions of the companies. And because the laws are consumer-centric, it allows for the businesses to rethink their approach, where they have to embed a "privacy-by-design" machinery to adequately comply with the terms of such regulations. This ensures an even playing field, where existing companies have to adapt to the newer norms and allows start-ups and newer businesses to integrate this concept since its inception. And based on the global trajectory observed since the introduction of the GDPR in 2018, there is indefinite growth for such regulations to arise from different states and their administrative bodies to further comply towards a standard global access in data protection practices.

CONCLUSION

The introduction of the GDPR and the DPDP Act has had an earnest outcome in terms of introducing a global understanding towards data security and privacy laws and its application is not restricted to any secluded form of business, but rather applies to any and all businesses engaging in any form of trade, which involves collection of data from their users. irrespective

of their size, age, and reputation, every business has to mandatorily apply these privacy laws provided to ensure an equally accessible global market. This introduces a wide array of opportunities as well as challenges for existing businesses, SMEs and start-ups. But the observation of applying these regulations prove that it is more than just legal compliance, but an opportunity to enhance their company's branding with a smooth user experience, increase customer trust and create a dynamic position for themselves. As the evolution of businesses is seen through the future complexities, it also allows for a forehanded approach towards adapting to said challenges, and the current adaptation towards privacy laws will pose to be an example on how businesses can pivot themselves to adapt to the digital age.

REFERENCES

Legislations and Books

- Directive 95/46/EC of the European Parliament and of the Council (1995)
- Regulation (EU) 2016/679 (General Data Protection Regulation) [2016] OJ L119.
- Digital Personal Data Protection Act 2023 (India).
    - Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press 2015).
    - Bygrave LA, *Data Privacy Law: An International Perspective* (Oxford University Press 2014).
    - Chander A, *The Electronic Silk Road: How the Web Binds the World Together in Commerce* (Yale University Press 2013).

Surveys and Reports

- European Commission, Impact of GDPR on European Businesses (2020) https://ec.europa.eu accessed 26 January 2025.
- NASSCOM, Digital Personal Data Protection Act: Implications for Indian Startups (2023) https://nasscom.in accessed 26 January 2025.
- Salesforce, Enhancing Privacy and Security Compliance for GDPR (Salesforce, 2019) https://www.salesforce.com accessed 26 January 2025.
- Reserve Bank of India, Data Protection Guidelines for Financial Institutions (RBI, 2023) https://rbi.org.in accessed 26 January 2025.
- Flipkart, Adopting DPDPA Compliance for Secure Transactions (Flipkart, 2023) https://flipkart.com accessed 26 January 2025.
- Autoriteit Persoonsgegevens, Dutch Hospital Fined for Poor Security Practices (AP, 2019) https://autoriteitpersoonsgegevens.nl accessed 26 January 2025.
- DuckDuckGo, Our Commitment to Privacy under GDPR (2018) https://duckduckgo.com accessed 26 January 2025.