

Privacy as a Competitive Advantage: How Robust Data Protection Laws Shape Global Economic Development, Comparative Analysis of Sri Lanka and European Union

Abeynaike S.W¹, Wickramanayake W.M.Y.S²

¹Attorney-at-Law, LL.M (Colombo) (Reading), LL. B (Colombo) (Hons.) Temporary Assistant Lecturer, Legal Studies Unit, Faculty of Management Studies and Commerce, University of Sri Jayewardenepura, Sri Lanka

²Attorney-at-Law, LL.M (Colombo) (Reading), LL. B (Colombo) (Hons.) Temporary Assistant Lecturer, Legal Studies Unit, Faculty of Management Studies and Commerce, University of Sri Jayewardenepura, Sri Lanka

DOI: <https://dx.doi.org/10.47772/IJRISS.2025.91200214>

Received: 22 December 2025; Accepted: 27 December 2025; Published: 06 January 2026

ABSTRACT

In recent years, the concern for data protection has moved beyond being a mere technical matter to becoming a legally enforceable obligation that requires timely and responsive actions by modern legal discourse; especially given the current rate of digitalization and use of artificial intelligence, coupled with increasing cross border data movements. Hence, this research aims to evaluate the current state of the EU and Sri Lanka's data protection legal frameworks with respect to their effect on economic development. Thus, this research focuses primarily on identifying and evaluating the legal and structural shortcomings of Sri Lanka's Personal Data Protection Act No. 09 of 2022 (PDPA) as significant legislation that represents a significant step forward. Furthermore, this research evaluates the impact of interconnected phenomena such as globalization, privatization and competition on the governance of personal data and privacy within increasingly digitalized and competitive markets. By using a qualitative desktop research approach, the research utilizes both primary and secondary sources including legislation, academic literature, policies, and online resources to compare the data protection regimes of the EU and Sri Lanka in order to examine the implications of developing issues associated with artificial intelligence. Ultimately, the goal of this research is to provide a detailed understanding of the current state of data protection law and its economic impact, while providing practical and contextually appropriate recommendations to address the identified shortcomings of the PDPA through lessons learned from the European Union's GDPR in order to improve Sri Lanka's digital economy and promote sustainable economic growth.

Keywords: Data Protection, GDPR, PDPA, AI, Economic Development

INTRODUCTION

Globalization expands the scope of competition, allowing companies across the globe to compete. Privatization also expands the scope for companies by allowing them to operate in areas once managed by the state to encourage efficacy and innovation. Collectively these two phenomena lead to fair competition that is beneficial for consumers as it provides affordability and variety of choices. However, they can also create unfair competition that harms the wellbeing of consumers and businesses impacting market dynamics and the way business and consumers engage in global economy.

Along with the change of global market dynamics through these phenomena, data protection has arisen as a contemporary and critical issue that is essential to be addressed. This research compares the European Union's General Data Protection Regulation of 2016 (GDPR) and Sri Lankan Personal Data Protection Act No. 9 of 2022 (PDPA) in order to conduct a critical analysis of legislations, and their contribution for economic growth. The research considered European Union (EU) as its comparative jurisdiction, since GDPR is widely regarded as the global benchmark for data protection and consumer safeguards. Additionally, PDPA was developed relying on

GDPR's obligations and goals to enable cross border data flow while enhancing economic development (Nanayakkara, 2024). PDPA was chosen to evaluate how effectively this new legislation handles the evolving complexities of data protection in a globalized world.

This research firstly, identifies how the interconnectedness among Globalization, Privatization and Competition has impacted modern commerce. Secondly, the research highlights how these phenomena have led to the issue of data protection and draws comparison with GDPR and PDPA to examine how a robust data protection legal framework can contribute to economic development. The research concludes by highlighting that while PDPA is a progressive step towards protection data, it needs to address its ambiguities and concerns to be more comprehensive in handling the impacts of Globalization, Privatization and Competition for sustainable economic growth.

METHODOLOGY

This research adopts a qualitative doctrinal methodology based on desk research to critically examine data protection laws as a component of modern commercial law. The study relies on both primary and secondary sources, including statutory instruments such as the European Union General Data Protection Regulation (GDPR) and Sri Lanka's Personal Data Protection Act No. 09 of 2022 (PDPA), as well as international instruments, journal articles, and websites. A comparative legal approach is employed to analyse how robust data protection frameworks operate as a competitive advantage in the European Union, while identifying legal, institutional, and structural limitations within the Sri Lankan framework that may hinder economic development. The research further incorporates a contextual analysis of globalization, privatization, competition, and emerging technologies such as artificial intelligence to assess their impact on data governance and commercial practices. Through statutory interpretation and comparative evaluation, the methodology enables a comprehensive assessment of the effectiveness of existing legal frameworks and supports the formulation of practical, context-specific recommendations aimed at strengthening Sri Lanka's data protection regime and promoting sustainable economic growth.

Impact of Globalization, Privatization, and Competition on Global Market Dynamics

Globalization underscores how evolving trade and technology has created connected and interdependent economies, cultures and societies worldwide. By allowing businesses to access new markets and engage in global production, it has reshaped modern commerce and enhanced economic growth (Nahalková and Tesárová, 2021). While the concept has many unifying factors, it also contains divisive effects like creating uniformity among cultures, challenging sovereignty of nations and deepening existing disparities among countries (Udu, 2016).

Additionally, privatization is the shift of government assets, services and functions to private companies, reducing state's role and influence. The transfer of power would lead services like education and healthcare to become more market-oriented impacting social welfare and economy. (Public-Private Partnership Legal Resource Center, 2024). Additionally, this process will increase competition as it boosts efficiency in previously state-owned business and lessens the government financial burden (Udu, 2016)

Moreover, competition is the rivalry among businesses trying to attract customers to maximize profits by offering better services and goods. This phenomenon is affected by economic, legal and behavioral factors, as it encompasses both tangible benefits and perceptions surrounding those offerings (Clark, 1925). Economics view this concept as an industry rivalry, whereas social scientists view it as a contest for market control (Udu, 2016).

Globalization, Privatization and Competition collectively enhance efficiency, productivity and societal welfare. Globalization provides access to global market and boosts global production, while Privatization increases productivity and competitiveness of formerly state-owned services. Competition drives for innovations and provides affordable goods and services, creating a consumer-friendly global marketplace with improved living standards (Udu, 2016)

Therefore, the interrelation between globalization, privatization and competition have increased cross border transfers and reduced trade barriers and free flow of capital, collectively reshaping global businesses (Udu,

2016). Moreover, it has impacted in digitized markets, where consumers expect affordable, diverse and convenient digital experience.

Collectively these phenomena have created a competitive, consumer oriented and innovative global economy. However, with the development of digital markets, and the wide sharing of personal data prompts concern surrounding data protection. Thus, protecting data is the key to maintaining trust, promoting fair competition, enabling sustainable digital trade development.

Privacy as an advantage

Privacy operates as a clear advantage in the modern data-driven economy because it strengthens trust between consumers and firms while supporting long-term social and economic value. Robust privacy protections give individuals meaningful control over their personal data, including how it is collected, used, stored, and shared, which increases confidence in engaging with digital services. When consumers trust that their data is protected through transparency, strong security measures, and enforceable rights, they are more willing to share information, enabling firms to deliver better and more innovative services. At the same time, companies benefit from enhanced consumer trust and reduced risks associated with data misuse and breaches. In this way, privacy functions not as a barrier to economic activity, but as a strategic advantage that promotes responsible data practices, consumer confidence, and sustainable growth of the data economy (Yale School of Management, 2021).

Data Protection as a contemporary issue

Data protection prevents sensitive personal data from being accessed and misused; this ensures that responsibility regarding collection, storage, usage and disposal of such information is exercised aligning with privacy guidelines (Hyseni).

The rise of Artificial Intelligence (AI) has led to safeguarding data and challenging privacy. AI is capable of handling massive databases and uses variety of ways to gather data, which results in potential misuse of data (Digital Ocean).

Therefore, it is evident that data protection has emerged as a contemporary issue due to the impacts of Globalization, Privatization, and Competition that are affecting the global market dynamics. The interconnection among these phenomena necessitates a robust data protection legal framework in a highly competitive and digitally driven global market.

The growth of digital landscape has given rise to electronic commerce (e-commerce) which depends on digital platforms to facilitate business to business, business to consumer among other types of transactions (Rahmi, 2022). Despite its convenience, e-commerce gives rise to significant issues related to data protection as it collects personal data such as names, passwords, and credit card numbers. These privacy concerns can undermine consumer trust and security, especially given the uncertainty in the digitalized world as to who bears responsibility for safeguarding this data, leaving consumers with limited control over how their data is used, and potentially affecting consumer sovereignty.

Big data is utilized as a corporate strategy by companies, for target marketing and to personalize services (Rahmi, 2022). necessitating robust data protection legislation that prevents misuse of such sensitive data. Regulations like the GDPR set a high standard, likewise, demand other jurisdictions to also develop a strong data protection regulation, to protect both consumers and businesses in e-commerce.

Impact of AI

With advancements in AI, businesses use AI technology to compete with one another. Nevertheless, in the absence of strong data protection, companies may access or abuse personal and confidential data resulting in unfair competition (Scheuerer, 2021). Moreover, unfair competition occurs when businesses lacking AI tools are unable to compete with those that have access to data through such tools. Therefore, regulations that protect data privacy and ensure the same opportunities in AI-driven markets are necessary for fair competition.

Sri Lanka has taken some efforts to address this situation from the Computer Crimes Act No. 24 of 2007, since it deals with the identification and prevention of computer crimes (Computer Crimes Act 2007, preamble) and stating the unauthorized access to a computer as an offence. (Computer Crimes Act 2007, s 3). However, it is evident that this is not robust enough to address the impact of AI compared to the European Union since they have introduced a robust regulatory framework for AI aiming to protect Fundamental Rights.

Moreover, this strong legal framework upholds economic development by proposing a stable and transparent commercial environment. Companies around the world are benefitted by these strong regulations, promoting innovations and investments. This enhances global market competitiveness, ensuring sustainable growth in AI-driven industries. (Lescrauwaet, Wagner, Yoon and Shukla, 2022). Therefore, Sri Lanka should also focus on implementing a robust regulatory framework for data protection concerning AI since the current PDPA 2022 doesn't address the issues regarding AI. Hence it limits the country's ability to go forward with the fast-moving world.

A Comparative Analysis Between Legal Framework in the European Union and Sri Lanka, and their impact on Economic development

Parallels and Merits of PDPA

The GDPR has reshaped data privacy on a global scale, setting a benchmark in protecting individuals' privacy rights in a data-driven world. GDPR extends its application beyond European Union, holding any organization dealing with EU residents' data accountable (General Data Protection Regulation (2016)/679, art 3). The PDPA also has extraterritorial application if an entity or person outside of Sri Lanka (SL) provides goods or services to persons in SL, or tracks behavior within SL (Personal Data Protection Act No 09 of 2022, s 2(1)). Although, both the Legislations apply extraterritorially, GDPR has used more clearer and direct terminology regarding its application. Both regulations reflect globalization's influence on commercial law, as businesses operate cross-border it demands consistent legal frameworks to adopt and address modern commercial issues like data privacy.

The GDPR and PDPA define personal data broadly, covering various aspects of individual's identity. Person data is defined as information identified or identifiable natural person: telephone number, email address among other things (General Data Protection Regulation (2016) / 679, Article 4).

Furthermore, the common merit of both regulations is ensuring transparency and accountability, since it requires data to be collected lawfully and transparently and used for specified purposes. Moreover, it requires the data to be accurate, store no longer than necessary and to protect with security measures. Additionally, the accountability requirement holds data controllers to maintain compliance with data protection framework which thereby promotes a system where data privacy is a priority (Kirk, 2022).

PDPA adopting a similar framework as the GDPR is a significant merit as it will facilitate fostering trust in the digital economy enabling businesses to succeed while safeguarding consumer privacy. Further, the PDPA's similar positioning as to data minimization reflects how the legislation attempts to strike a balance between companies that rely on personal data with the privacy rights of whose data is being used, which is essential for economic growth as it has intricately provided a platform in navigating such issues while facilitating sustainable business practice in a globalized market.

Evidently, both the GDPR and PDPA reflect globalization's influence on data privacy laws, highlighting the necessity in ensuring a balance between economic growth with protection of personal data rights. GDPR recitals 2 and 5 among others, underscores how globalization has influenced shaping data protection standards that secure cross-border personal data flows, that support economic integration (European Parliament & Council of the European Union, 2016). Similarly, PDPA Preamble strives to promote the growth of innovation and digital economy while protecting the personal data rights of Data Subjects (Parliament of Sri Lanka, 2022). In respect to these foundational purposes, both the PDPA and GDPR offer similar rights to data subjects such as right to access, withdraw consent, rectification and erasure. This will allow individuals to have control over their personal data while transparency and accountability is exercised by data controllers.

Hence, both legislations enhance data privacy, promote responsible data handling, boosts consumer confidence and facilitate cross border transfers which improve economic growth. They also promote fair competition by enforcing a uniform and strong data protection standards to prevent misuse of consumer data to gain unfair advantage over the other.

Therefore, PDPA has strived to stay on par with the GDPR by promoting efficient and secure business operations for sustainable economic growth. It also portrays how data privacy has become a central element in business strategies and modern commerce, that impacts competition among companies and consumer engagement, influencing how business operates personal information and interacts with consumers.

Differences and shortcomings of PDPA

One of the major criticisms of the PDPA is the vagueness of the language, which could discourage foreign investment hindering economic development (Abeysekara & Ranasinghe, 2022). In contrast, GDPR offers a comprehensive framework that makes EU a desirable location to strengthen its competitiveness in the global market.

An instance that illustrates ambiguity of the PDPA is about its application. Both GDPR and PDPA exclude the processing of personal data for purely personal and household activities (General Data Protection Regulation (2016)/679, art 2(2)). However, apart from personal and household activities PDPA stipulates that act does not apply to “any data other than personal data” (Personal Data Protection Act, 2022, s. 2(3)(b)). This creates vagueness as even the interpretation section does not explain what it is meant by any data, leading to foreign companies and investors handling personal data to question regarding the protection granted by the PDPA, slowing economic growth.

Moreover, when considering the terminology used in the Acts, GDPR has defined the term anonymise in a more comprehensive and pragmatic manner. PDPA defines “anonymise” as permanently removing data making it impossible to trace any data (Personal Data Protection Act, 2022, s. 56), while GDPR uses the term “pseudonymisation” which allows to preserve data and trace additional information where necessary (European Union, 2016, art. 42(3)). The GDPR’s approach relating to anonymous data allows entities to use personal data such as patient data for the development of healthcare catering to the advancement of such sectors. This is also crucial to face unforeseen situations like the Covid-19 pandemic, as the preserved data can be used to innovate vaccines and other effective medicines. This aligns with the objectives of the preamble and recitals of both the legislations as it facilitates a practical and sustainable strategy to protect data while contributing to economic development.

The PDPA imposes strict obligations on both data controller and processor. The data processor’s non-compliance with conditions on processing leads to penalties. This is a major difference when compared to GDPR, which reserves such obligations primarily to the controller. This approach may raise regulatory burdens on data processors, discouraging investment in data processing and outsourcing industries, hindering economic development (Abeysekara & Ranasinghe, 2022).

Both the GDPR and PDPA provide rights to individuals regarding automated decisions. While both acts stipulate similar exceptions, PDPA allows an individual to request and review if an automated decision has irreversible and continuous impact, whereas GDPR allows for legal and significant effects. The literal interpretation of GDPR offers wider protection by covering more situations in which data subjects may be exempted from automated decision making (Nanayakkara, 2024). In the age of Globalization, AI and automated processes has become integral to global competition. Hence, the GDPR’s broader approach to automated processes make the EU attractive to business seeking strong data protection to ensure consumer trust, leading to growth in its economy. Conversely, the PDPA’s narrow application may deter foreign investments as it fails to adequately address the growing technological concerns, hindering economic development.

Furthermore, PDPA fails to establish an independent Data Protection Authority (DPA) which could severely impact economic development. The government can potentially control the authority by issuing directions leading businesses and investors to question the legitimacy and impartiality of enforcement of data protection standards. This opposes principles like transparency, in GDPR as it suggests that the supervisory authority

established must be an independent public body (Abeysekara & Ranasinghe, 2022). This could weaken investor's confidence and hinder technological innovation, creating inefficiencies as it lacks the independence essential for smooth operation, hindering SL's economic growth.

PDPA, similar to GDPR, allows data controllers to conduct Data Protection Impact Assessment (DPIA), when the processing is likely to result in high risks to the rights of the data subjects (General Data Protection Regulation [GDPR], 2016, art. 35). Additionally, the PDPA requires the controller to submit the DPIA to the DPA (European Union, 2016, art. 35) making the process more time consuming. This will delay the delivery of innovative products and services, making SL less competitive in the global market.

Further, unlike the GDPR, the PDPA does not mention regular reviews to assess whether processing is performed in accordance with DPIA when there is a change of the risk represented by the processing operations (General Data Protection Regulation [GDPR], 2016, art. 35). This will prevent us from ensuring that businesses remain adaptable to evolving risks and global market conditions, slowing the economic growth in SL.

Globalization has given rise to increase growth of cross border data flows, which are fundamental to international trade and business, and forms as a backbone in modern economy. Unlike the GDPR, the PDPA requires that personal data processed by public authorities in SL to be stored within the country, unless the DPA allows otherwise. Hence, Companies providing services to the government may face increased costs due to the need to store data locally in SL. The PDPA, unlike the GDPR, does not allow data transfers based on user consent, limiting flexibility in data sharing (Abeysekara & Ranasinghe, 2022). These restrictions would create inefficiencies and additional costs for companies operating in the global market. In contrast, the GDPR's transparent and clear standards provide companies with an environment that is secure and smooth for cross border operations. Moreover, this regulation certainly reflects how EU has complied with the changing dynamic in the global marketplace, where strong data protection regulations are playing an important role in economic development. Hence, SL should also adhere to such changes accordingly to accelerate its economic growth.

Accordingly, globalization facilitates the constant transfer of data across borders which is essential for business operation, increasing the risk of data breaches. While privatization can lead to transfer of data-oriented services from the public domain to private sector raising concerns about data privacy and security. For instance, Healthcare organizations that heavily rely on patient's data may compromise such data to gain profits. Further, companies will utilize AI for innovations and to provide valuable insights into marketing trends which gives businesses a competitive edge. Lack of robust data protection leads to companies misuse personal and confidential data for competitive advantage, creating disparity between large and small-scale business. This will envitably result in unfair competition as large-scale businesses can access sensitive data and misuse such data to refine their strategies and utilize sophisticated algorithms (Mohamed, 2021) that can better evaluate customer engagement.

Implementing effective data protection regulations will ensure fair competition as it will allow equal opportunity to businesses in a data driven global economy. Thus, it highlights the crucial role of data protection laws and the necessity of such laws to be strong and comprehensive, to carefully address the impacts of globalization, privatization and competition and ensure that benefits of these phenomena do not come at the expense of consumer privacy.

CONCLUSION

In conclusion, phenomena such as Globalization, Privatization, and Competition encompass both collective and individual effects. The concepts have collectively impacted modern commercial law by changing its dynamics to tackle contemporary issues such as data protection and also impacts consumers by risking and increasing their vulnerability as to personal data.

Privacy is recognized as fundamental human rights in Universal Declaration of Human Rights and International Covenant on Civil and Political Rights (Abeysekara & Ranasinghe, 2022), highlighting that mere recognition of data protection is insufficient and necessitates a comprehensive legal framework to protect personal data. Prior

to the PDPA, various legislations like the Computer Crimes Act of 2007 were used to protect data through its implied application (Abeysekara & Ranasinghe, 2022).

The rise of AI has also made the process of data protection more complex. Thus, portraying data protection as a contemporary issue as its evolvement, presents emerging aspects surrounding it. In response, EU has introduced the AI Act to respond to these concerns alongside the protection guaranteed by the GDPR.

Nevertheless, PDPA can be considered a significant milestone that addresses the long overdue need to handle data protection and privacy. However, although there are a considerable number of merits to the act, it can be recommended to address the aforementioned issues relating to ambiguity and other concerns, while also adopting its law to identify their specific needs. Also, to articulate their laws while learning lessons from the experiences of other countries, to boost economic growth (Abeysekara & Ranasinghe, 2022).

REFERENCE

Legislation

1. Personal Data Protection Act, No. 9 of 2022 (Sri Lanka).
2. European Union. (2016). General Data Protection Regulation (EU) 2016/679. <<https://eur-lex.europa.eu/eli/reg/2016/679/oj>>

Journal Articles

1. Abeysekara, T. B., & Ranasinghe, A. E. (2022). Holistic approach in introducing proper legal framework to regulate data protection and privacy in Sri Lanka. *Vidyodaya Journal of Management*, 8(1). <<https://vjm.sljol.info/articles/89>>
2. Clark, J. M. (1925). What is competition? *Journal of Political Economy*, 33(3). <<https://www.jstor.org/stable/2354777>>
3. Nahalková, E., & Tesárová, A. (2021). The impact of globalization in connection with the development of e-commerce. *SHS Web of Conferences*, 92, Article 06007. <https://www.shsconferences.org/articles/shsconf/abs/2021/40/shsconf_glob2021_06007/shsconf_glob2021_06007.html>
4. Nanayakkara, T. (2024). An analysis of privacy policies in Sri Lanka. *University of Colombo Review (Series III)*, 5(21). <<https://ucr.sljol.info/articles/158/files/6671137745092.pdf>>
5. Scheuerer, S. (2021). Artificial intelligence and unfair competition – Unveiling an underestimated building block of the AI regulation landscape. *GRUR International*, 70(9). <<https://academic.oup.com/grurint/article/70/9/834/6178541>>
6. Udu, A. A. (2016). Globalisation, privatisation and competition in the third world countries. *International Journal of Business and Social Science*, 7(4), 79–86. <https://ijbssnet.com/journals/Vol_7_No_4_April_2016/8.pdf>

Reports

1. Lyytinen, J., Lescrauwet, B., Hekkert, M., Wagner, C., Cheng Yoon, A., & Sovacool, B. K. S. (2022). Adaptive legal frameworks and economic dynamics in emerging technologies: Navigating the intersection for responsible innovation. <https://www.researchgate.net/publication/375988655_Adaptive_Legal_Frameworks_andEconomic_Dynamics_in_Emerging_Technologies_Navigating_the_Intersection_for_Responsibile_Innovation>

Web Pages

1. DigitalOcean. (n.d.). AI and privacy: Safeguarding data in the age of artificial intelligence. <<https://www.digitalocean.com/resources/articles/ai-and-privacy>>
2. Hyseni, V. (n.d.). Data protection challenges. PECB. Retrieved November 15, 2024, from <<https://pecb.com/article/data-protection-challenges>>

3. Kirk, N. (2022, March 30). Sri Lanka becomes the first South Asian country to pass comprehensive privacy legislation. WilmerHale. <<https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20220330-sri-lanka-becomes-the-first-south-asian-country-to-pass-comprehensive-privacy-legislation>>
4. Public-Private Partnership Legal Resource Center. (2024, October 11). Privatization laws. <[https://ppp.worldbank.org/public-private-partnership/legislation regulation/laws/privatization](https://ppp.worldbank.org/public-private-partnership/legislation-regulation/laws/privatization)>
5. Yale School of Management. (2021, January 15). The benefits of privacy. Yale Center for Customer Insights. <<https://som.yale.edu/blog/the-benefits-of-privacy>>