Indonesia Law Collage Association Law Journal (ILCA Law Journal)
ISSN : 2963-3621 (online)_____VOL 3 NO 2 DECEMBER 2024

Comparative Analysis of Indonesia's Personal Data Protection Law with the European Union and California Regulations to Identify Best Practices in Protecting Public Privacy Rights

Muhammad Maleno[1*], Andriana Kusumawati[2]
[1,2]Sekolah Tinggi Ilmu Hukum IBLAM, Jakarta, Indonesia
malenom.mm@gmail.com[1*], andriana@gmail.com[2]

Abstract

Personal data protection has become a critical issue in the digital era, as data breaches increase in Indonesia. Law No. 27 of 2022 concerning Personal Data Protection (PDP Law) is a newly enacted regulation aimed at safeguarding individuals' privacy rights. However, the implementation of the PDP Law still faces various challenges, especially in terms of law enforcement and oversight of electronic system providers. This research aims to analyze the substantial differences between Indonesia's PDP Law, the European Union's General Data Protection Regulation (GDPR), and the United States' California Consumer Privacy Act (CCPA), as well as to identify best practices that can be adopted to strengthen personal data protection in Indonesia. This study employs a normative legal research method with a statutory and comparative approach. An analysis of GDPR and CCPA, both recognized as global standards for data protection, is conducted to provide recommendations for enhancing Indonesia's regulations. The results indicate that while the PDP Law is a positive step, there are still weaknesses in terms of transparency, accountability, law enforcement, and the granting of data subject rights. Indonesia can adopt practices from the GDPR, such as data protection impact assessments and stricter sanctions, as well as from the CCPA in giving consumers greater control over their data. This study recommends improving law enforcement mechanisms, transparency in data management, and public education on the importance of personal data protection. By referring to effective international regulations, Indonesia can enhance the effectiveness of its PDP Law and strengthen the protection of privacy rights in the increasingly complex digital era.

Keywords : Personal Data Protection, Europe, California, Regulation

INTRODUCTION

Personal data protection in Indonesia has become a growing concern as data leaks have increased in recent years. Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) is a significant step taken by the government to protect people's privacy rights. However, the implementation of this regulation still faces various challenges, especially in law enforcement and supervision of electronic system organizers. Cases of massive data leaks that have occurred, such as those involving BPJS Kesehatan and the General Election Commission (KPU), show weaknesses in cybersecurity in important sectors (Handayani, 2023). These data leaks not only endanger individuals' privacy rights but also create public distrust of digital service providers (Prabowo, 2022).

One of the most prominent data leak cases was the BPJS Kesehatan data leak in 2021, where data of more than 279 million Indonesians was traded on illegal online forums. In addition, the KPU data leak in the 2019 election which exposed voter data was also in the spotlight. This case shows the weakness of cybersecurity infrastructure in government institutions, which are the main targets of hacking (Iskandar, 2021). Another case that occurred was the Tokopedia and Bukalapak data leak, which endangered millions of users on the e-commerce platform. With these many incidents, experts argue that regulatory enforcement efforts and awareness of the importance of data protection must be increased (Sutrisno, 2022).

The PDP Law has not fully provided optimal protection, because there are still gaps in handling personal data breaches. Many parties are concerned about the lack of coordination between the government and the private sector in implementing this regulation (Lestari, 2023). Several experts argue that law enforcement against data leaks is still weak and is often not accompanied by strict sanctions against perpetrators of violations, both electronic system organizers and parties who misuse data. Therefore, it is necessary to improve technological capabilities, law, and public awareness to face this challenge effectively.

Personal data protection in developed countries such as the European Union and the United States is already regulated by strict regulations, such as the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. GDPR is one of the most comprehensive personal data protection regulations in the world, which gives individuals greater rights over their data and imposes severe sanctions on companies that violate it. GDPR sets out basic principles such as transparency, accountability, and the right to be forgotten, which protect users from data misuse. Meanwhile, the CCPA in California gives consumers the right to know what information is collected by companies, and allows them to request data deletion and opt out of the sale of personal data.

This research is important because by comparing regulations in Indonesia with GDPR and CCPA, we can identify best practices that can be adopted to strengthen personal data protection in Indonesia. Currently, Indonesia is still in the early stages of implementing the Personal Data Protection Law (Law No. 27 of 2022), which although significant, still has much room for improvement, especially in law enforcement and oversight of data misuse. By studying how other countries manage personal data, this research can provide insights for policymakers to improve the effectiveness of privacy protection in the ever-evolving digital era. The formulation of the problem in this research is how are the substantial differences between the Indonesian Personal Data Protection Law and the GDPR regulations in the European Union and the CCPA in California in protecting people's privacy rights? And what are the best practices from the GDPR and CCPA regulations that can be adopted by Indonesia to improve the effectiveness of personal data protection and people's privacy rights?

This study uses a normative legal research method, which focuses on the study of written legal norms and principles that apply in personal data protection regulations, both in Indonesia and in other countries such as the European Union and the United States. Normative

legal research is conducted with a statute approach and a comparative approach, where the applicable legal regulations in Indonesia, namely Law No. 27 of 2022 concerning Personal Data Protection, will be compared with the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. This makes it possible to identify the advantages and disadvantages of each regulation in the context of personal data protection (Marzuki, 2017). This study will also analyze various literature and legal documents to understand the effectiveness and challenges of implementing existing regulations (Soekanto, 2019).

RESEARCH METHODS

This study also uses a conceptual approach, namely by exploring legal concepts relevant to the protection of privacy rights and data surveillance in the digital era. Secondary data in the form of scientific journals, books, and legal reports will be the main materials in this study. This literature study is needed to understand the development of law in the field of personal data protection and to examine how data protection principles are implemented in various jurisdictions (Hatta, 2020). Through this normative legal method, this study aims to provide relevant policy recommendations for improving regulations in Indonesia, taking into account experiences from other countries (Friedman, 2018).

RESULT AND DISCUSSION

Comparison of Law Number 27 of 2022 Concerning Protection of Indonesian Personal Data with the General Data Protection Regulation and the California Consumer Privacy Act in Protecting People's Privacy Rights

Personal data protection is increasingly becoming a global concern, especially with the development of information technology and digitalization. In Indonesia, Law No. 27 of 2022 concerning Personal Data Protection (UU PDP) is a major step in efforts to protect people's privacy rights. This law is designed to provide legal protection for the collection, processing, and storage of personal data by various parties, both state and private institutions. On the other hand, two international regulations, the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, are often considered global standards in data protection (Kuner, 2020; California State Government, 2018). In comparing these three regulations, it is important to explore various aspects such as scope, individual rights, and sanctions and supervision regulated in each regulation.

The Indonesian Personal Data Protection Law has a broad scope, covering all electronic and non-electronic personal data held by both public and private bodies. Similar to the GDPR, the Indonesian PDP Law also regulates the rights of data subjects, such as the right to access, correct, and delete their personal data. However, compared to the GDPR, the scope of individual rights in the Indonesian PDP Law is still not as comprehensive as the GDPR. The GDPR provides further rights such as the right to data portability and the right not to be subject to decisions taken based on automated data processing, which are not fully accommodated in the PDP Law.

One of the advantages of GDPR is its emphasis on clear data processing principles, such as transparency, accountability, and data minimization. These principles form the basis for the collection and processing of personal data in the European Union. GDPR also requires data controllers to conduct a Data Protection Impact Assessment (DPIA) before processing sensitive or high-risk data. In Indonesia, although these principles are also adopted in the PDP Law, their implementation is not as strong and strict as that stipulated in the GDPR. This is one of the main weaknesses of the Indonesian PDP Law, which still needs strengthening in terms of implementation and supervision.

The CCPA focuses more on consumers' rights to know what information companies collect, and gives them control over that data. The CCPA gives consumers the right to request that their personal data not be sold to third parties. This differs from the GDPR, which focuses more on general data processing principles than specific rights related to data sales. Indonesia's PDP Law is closer to the GDPR in terms of general data processing principles, but lacks the CCPA's specific focus on consumer data.

In terms of enforcement, GDPR has a very strong mechanism. Data regulators in the European Union, such as the Information Commissioner's Office (ICO) in the UK, have the authority to impose very high fines on companies that violate GDPR. Fines can reach up to 4% of a company's total global revenue, which is a strong incentive for companies to comply with the rules. In Indonesia, the PDP Law also provides quite strict sanctions, including administrative and criminal fines. However, the amount of the fines and the enforcement mechanisms are still not as strong as GDPR. This is a challenge for Indonesia in ensuring company compliance with data protection regulations.

CCPA has lower fines than GDPR, and also gives consumers the right to sue companies that violate their rights in terms of data protection. This is one of the advantages of CCPA which strengthens the position of consumers in protecting their privacy rights. The Indonesian PDP Law, although it regulates the right to sue, still does not provide a clear mechanism on how data subjects can sue companies that violate their rights. In this case, the Indonesian PDP Law needs to learn from CCPA in strengthening the law enforcement aspect for data subjects.

Supervision and control are also striking differences between the three regulations. GDPR has an independent agency tasked with overseeing compliance with the rules, while CCPA has a special agency tasked with monitoring violations of consumer rights related to data. Article 63 of Law No. 27 of 2022 concerning Personal Data Protection states: "The state administrator authorized in the field of personal data protection is the government administrator in charge of communications and informatics."

In terms of transparency, the GDPR and CCPA have high standards when it comes to notifying data subjects about how their data is processed. The GDPR, for example, requires companies to provide clear and easy-to-understand information to users about how their data is used (European Commission, 2018). In Indonesia, the PDP Law also regulates this notification obligation, but the level of transparency still needs improvement to be in line with GDPR standards (Law No. 27 of 2022, Article 52).

Another advantage of the GDPR is the obligation for data controllers to report data breaches to the supervisory authority and data subjects within 72 hours of the breach being discovered. This provides additional protection for data subjects, as they can take immediate action upon learning of a data breach (European Commission, 2018, Articles 33 and 34). In Indonesia, the obligation to report data breaches is also regulated in the PDP Law, but the deadline is still looser than the GDPR, which has the potential to reduce the effectiveness of protecting data subjects (Law No. 27 of 2022, Article 63). Meanwhile, the CCPA in California also regulates the obligation to notify consumers within a longer period than the GDPR, with a deadline of 45 days after the data breach is discovered (California State Government, 2018, Article 1798.82).

Implementation One of the main shortcomings of the Indonesian PDP Law is the absence of a strong framework for data protection impact assessment as regulated in the GDPR. This assessment is important to ensure that any high-risk data processing does not have a negative impact on data subjects. Indonesia needs to learn from the GDPR in this regard to strengthen the risk prevention and management aspects.

The amendment to Indonesia's PDP Law is a positive step in strengthening personal data protection, but there are still some weaknesses that need to be addressed. Strengthening the oversight and law enforcement mechanisms, as well as increasing transparency and

accountability in data processing, are key to optimizing data protection in Indonesia. Compared to the GDPR and CCPA, Indonesia's PDP Law is still in its early stages of development. The GDPR offers stricter standards and more severe sanctions, while the CCPA gives consumers greater power to control their personal data. Indonesia's PDP Law needs to accommodate these strengths to improve privacy protection in an increasingly complex digital era.

Identifying Best Practices from GDPR and CCPA to Improve the Effectiveness of Personal Data Protection in Indonesia

Personal data protection is a very important issue in the digital era. In various countries, regulations related to data protection have been implemented to protect people's privacy from the threat of data leaks and misuse. In Indonesia, this effort is carried out through Law No. 27 of 2022 concerning Personal Data Protection (UU PDP). However, to increase its effectiveness, Indonesia can learn from the best practices implemented in the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States. These two regulations are known as international standards in terms of personal data protection, with different but complementary approaches (European Commission, 2018; California State Government, 2018; Law No. 27 of 2022).

One of the best practices taken from the GDPR is the emphasis on the principles of transparent, accountable, and consent-based data processing. The GDPR requires data controllers to clearly inform data subjects about the purpose of their data collection, how the data will be used, and who will have access. This transparency principle gives data subjects greater control over their personal information (European Commission, 2018). In Indonesia, the PDP Law also regulates the same thing, namely the obligation to notify data subjects about the purpose of collecting and using personal data. However, the monitoring and enforcement mechanisms are still not as strong as the GDPR. The PDP Law stipulates that the personal data supervisor is under the Ministry of Communication and Information, but in practice, the implementation of monitoring and law enforcement still needs to be strengthened to be effective as regulated in the GDPR (Law No. 27 of 2022, Article 63). Indonesia can adopt stricter monitoring and an independent audit mechanism to ensure that this transparency runs well.

Another advantage of the GDPR is the obligation for data controllers to conduct a Data Protection Impact Assessment (DPIA) before processing sensitive or high-risk data. This aims to identify and mitigate potential risks to the privacy and rights of data subjects (European Commission, 2018, Article 35). This DPIA is an important tool in preventing the risk of data leakage, as it requires companies to conduct an in-depth risk analysis and implement appropriate precautions. Indonesia can learn from this GDPR by introducing stricter DPIA obligations, especially for large companies that handle sensitive or large amounts of data.

The GDPR provides very strong rights to data subjects, including the right to access data, correct incorrect data, and erase their data (right to be forgotten) (European Commission, 2018, Articles 15, 16, 17). These rights provide significant protection for individuals from data misuse. In Indonesia, these rights are already regulated in the PDP Law, but its implementation is not as strong as in Europe. Strengthening the complaint management system and mechanisms for data subjects to submit requests regarding their data should be a top priority in increasing the effectiveness of the PDP Law. On the other hand, the CCPA provides a more focused approach to consumer rights, especially in terms of access to their data and the ability to prevent data from being sold to third parties. This is different from the GDPR which emphasizes more on general principles of data processing. The best practice from the CCPA that Indonesia can adopt is to give data subjects more control over how their data is used in commercial activities, including the right to refuse the sale of data. Indonesia needs to specifically regulate how

personal data is traded and require companies to obtain explicit consent from data subjects before selling the information.

In terms of fines and sanctions, the GDPR imposes very high fines for violators, up to 4% of a company's annual global revenue or 20 million Euros, whichever is higher. These stringent sanctions put pressure on companies to comply with data protection regulations. In Indonesia, although the PDP Law also stipulates administrative and criminal sanctions, the level of fines imposed is not yet comparable to the GDPR. Indonesia could introduce more significant fines, especially for large companies that violate data protection provisions, to ensure stronger compliance. The CCPA also emphasizes the importance of notifying consumers in the event of a data breach. Under the CCPA, companies are required to notify consumers within a certain time frame if there is a personal data breach. Indonesia could adopt similar provisions, shortening the deadlines set out in the PDP Law for reporting data breaches, to minimize the impact of the breach and allow data subjects to take necessary protective measures.

In terms of supervision, GDPR has a strong independent institution, such as the European Data Protection Board (EDPB), which is responsible for enforcing the rules and providing technical guidance to member states. Indonesia, in the PDP Law, In the PDP Law, the authority to supervise personal data protection is given to government administrators in charge of communications and informatics as supervisory authorities, but this authority needs to be strengthened with adequate resources and authority. To improve the effectiveness of supervision, Indonesia can consider establishing an independent institution that specifically handles personal data protection and has the authority to conduct investigations and audits of companies.

Another best practice from the CCPA that can be adopted is the consumer's right to refuse the collection of their personal data on websites or digital applications, commonly known as "do not track." With the increasing prevalence of online data collection through cookies and other tracking tools, regulations in Indonesia must start to regulate these data collection practices more strictly. The PDP Law can be updated to require websites and applications to provide clear options for users to refuse the collection of their data or the sale of their information to third parties.

One of the challenges faced by Indonesia in implementing the PDP Law is the lack of public awareness regarding the importance of personal data protection. Best practices from the GDPR and CCPA can be implemented by educating the public about their rights as data subjects. For example, the GDPR provides very detailed guidance on the rights of data subjects and the obligations of data controllers, which are disseminated through public awareness campaigns. Indonesia needs to implement a similar education program, involving various parties, including the government, private sector, and civil society.

This study shows that although the PDP Law has been well-designed, there are still many aspects that need to be improved to meet the global standards applied in the GDPR and CCPA. One of the main priorities is strengthening the law enforcement mechanism, including stricter supervision and heavier sanctions. In addition, aspects of transparency and accountability in data management also need to be improved to ensure that people's privacy rights are well protected. These two international regulations also provide important lessons on the importance of privacy protection in the increasingly digital era. Regulations related to data sales and violation notifications, as regulated in the CCPA, as well as the obligation to conduct DPIA and provide strong rights to data subjects, as regulated in the GDPR, are things that Indonesia must consider in strengthening the PDP Law.

Best practices from GDPR and CCPA provide a clear picture of how personal data protection can be implemented effectively. Indonesia needs to take more proactive steps in improving existing regulations, ensuring that people's privacy rights are protected from the

threat of misuse and data leaks that are increasingly rampant in the digital era. The next step is to evaluate the implementation of the PDP Law in the field, and revise articles that do not meet data protection needs in Indonesia. This can be done by referring to international regulations that have been proven effective, such as GDPR and CCPA, to ensure that the PDP Law is able to provide adequate data protection in this digital era.

CONCLUSIONS

The conclusion of the comparison between the Indonesian Personal Data Protection Law with the GDPR and CCPA shows that although Indonesia already has a legal basis through Law No. 27 of 2022, there are several important aspects that need to be strengthened. The GDPR provides more comprehensive protection related to transparency, accountability, and data subject rights, while the CCPA focuses on consumer control over their personal data. Both regulations offer best practices that can be adopted by Indonesia, such as the application of heavier fines for violations, mandatory data protection impact assessments, and more independent and strict oversight mechanisms.

This study also underlines that to improve the effectiveness of personal data protection in Indonesia, it is necessary to strengthen law enforcement, public education, and increase transparency in data management. The PDP Law must be more adaptive to the challenges of the ever-evolving digital era, by considering more solid protection mechanisms than GDPR and CCPA. Personal data protection is not only a regulatory requirement, but also a basic right of every individual that must be maintained to ensure the security of people's privacy in the digital world.

REFERENCES

Alamsyah, B. (2020). *Personal data protection in the digital era*. Jakarta: Gramedia Pustaka Utama.

Andini, W. (2021). Comparison of GDPR and CCPA from the perspective of personal data protection. *Journal of Law and Justice, 7*(2), 120–135.

California Consumer Privacy Act (CCPA) of 2018. (2018). Retrieved from https://oag.ca.gov/privacy/ccpa

Darmawan, R. (2019). *Law and information technology: Personal data protection regulations*. Yogyakarta: UGM Press.

Fadli, Z. (2023). Effectiveness of personal data protection policies in Indonesia after Law No. 27 of 2022. *Journal of Legal Studies, 5*(3), 90–105.

Friedman, G. (2018). *Privacy, data protection, and the law: A global perspective*. Cambridge University Press.

Friedman, L. M. (2018). *The legal system: A social science perspective*. Russell Sage Foundation.

General Data Protection Regulation (GDPR) 2016/679. (2018). European Commission. Retrieved from https://eur-lex.europa.eu

General Data Protection Regulation (GDPR), Article 35: Data Protection Impact Assessment (DPIA). (2018). Retrieved from https://gdpr-info.eu/art-35-gdpr/

Hakim, S. (2021). *Data privacy and security: Challenges of the digital era*. Bandung: Alfabeta.

Handayani, A. (2023). Challenges of personal data protection in Indonesia post-major data breach. *Research Report, Center for Technology and Law Research*.

Handayani, N. (2023). BPJS Kesehatan and General Election Commission data leaks: Challenges in personal data protection in Indonesia. *Journal of Cyber Security, 15*(2), 45-60.

Hartono, D. (2020). Analysis of personal data protection policies in Indonesia based on global practices. *Journal of Technology Law, 4*(1), 45–59.

Hatta, M. (2020). *Personal data protection in the digital era: International and national legal perspectives*. Jakarta: Universitas Indonesia Publisher.

Indrawati, S. (2022). Data protection law enforcement mechanisms in Indonesia: Lessons from GDPR. *Journal of Law and Policy, 6*(1), 72–85.

Iskandar, B. (2021). Case study of BPJS Kesehatan and KPU data leaks. *Indonesian Data Security Journal, 7*(4), 198-211.

Kuner, C. (2020). *The General Data Protection Regulation: A commentary*. Oxford University Press.

Law No. 27 of 2022 concerning Personal Data Protection.

Lestari, P. (2023). The role of government in ensuring personal data security in Indonesia. *Journal of Public Administration, 13*(2), 210-225.

Lestari, R. (2023). Coordination between government and private sector in implementing the Personal Data Protection Law. *Journal of Law and Technology, 19*(1), 34-49.

Marzuki, P. M. (2017). *Legal research*. Jakarta: Kencana.

Mulyono, A. (2022). *Cyber law and privacy policy in Indonesia*. Surabaya: Airlangga University Press.

Nugroho, E. (2021). Personal data protection policy in the context of the digital economy in Indonesia. *Journal of Digital Economy, 8*(2), 155–170.

Prabowo, D. (2022). The impact of data leaks on public trust in digital services. *Journal of Technology and Privacy, 10*(4), 85-99.

Prabowo, D. (2022). Data leaks and their impact on public trust. *Indonesian Cyber Security Journal, 5*(1), 45-56.

Prasetyo, B. (2019). *Legal aspects of personal data protection in electronic information systems*. Jakarta: Kencana.

Soekanto, S. (2019). *Introduction to legal research*. Jakarta: Rajawali Press.

Suryanto, D. (2023). Protection of privacy and personal data in the digital era: A critical review of Law No. 27 of 2022. *Journal of Law and Information Technology, 9*(2), 101–120.

Sutrisno, B. (2022). Data leakage analysis on e-commerce platforms: The cases of Tokopedia and Bukalapak. *Journal of Data Protection and Technology, 7*(3), 77-91.

Sutrisno, R. (2022). Personal data security and its protection in the digital era. *Journal of Technology Law, 10*(2), 123-138.