Lentera Hukum, 12:1 (2025), pp. 42-61
ISSN 2355-4673 (Print) 2621-3710 (Online)

Available online 30 April 2025
https://doi.org/10.19184/ejlh.v12i1.47621

Research Article

Evaluating Data Breach Notification Protocols: Comparative Analysis of Indonesia and South Korea

Ampuan Situmeang*
Universitas Internasional Batam, Indonesia

Jihyun Park
Youngsan University, Korea

Lu Sudirman
Universitas Internasional Batam, Indonesia

Ninne Zahara Silviani
Universitas Internasional Batam, Indonesia

Shenti Agustini
Universitas Internasional Batam, Indonesia

ABSTRACT: Data protection is one of the most important aspects of the digital economy, with its legal implications extending across digital landscapes. The failure to protect data in data breaches can threaten the interests of owners and expose them to various risks. Legal compliance regarding how owners are notified of data breaches is important to prevent this, necessitating deep legal discourse and analysis. Using a comparative legal research method with a statutory approach, this study dissects norms within Indonesia and South Korea's legal systems to analyze their differences in legal compliance regarding this issue. The findings of this study highlight the discrepancies in legal frameworks between Indonesia and South Korea. It particularly notes Indonesia's lack of a governing body for data breach notifications and the absence of comprehensive privacy impact assessments or cybersecurity compliance. Ultimately, the study underscores the need for Indonesia to develop a normative model for data protection to address its significant regulatory gaps—contrasting with South Korea's more robust legal mechanisms and the GDPR's systematic oversight.

KEYWORDS: Data Breach, Data Breach Notification, Data Protection.

*Corresponding author, email: ampuan.situmeang@uib.ac.id

Submitted: 23 April 2024 | **Reviewed**: 28 April 2025 | **Revised:** 5 May 2025 | **Accepted**: 14 May 2025

I. INTRODUCTION

Digital technologies have driven data generation to grow amazingly, creating unprecedented opportunities and challenges.[1] The relevant digital technologies are created to improve connectivity, shifting the landscape of how people communicate and carry out daily activities.[2] Data has become an important commodity in today's economy, sometimes surpassing the value of traditional resources.[3] This has put data protection to the forefront of legal and ethical discourse. Indonesia and South Korea are prominent players in the development of the digital economy within the Asia-Pacific region.[4] The changes have significantly revolutionized many economies, giving birth to what is referred to as the fourth industrial revolution, or "Industry 4.0."[5] Both countries have benefited from the utilization of digital technology as the core aspect of Industry 4.0,[6] which is an umbrella concept encompassing a broad range of increasingly digital and connected technologies and applications-such as physical-digital interfaces, network and data-processing technologies-characterized by virtualization, real-time information sharing, and autonomy aimed at achieving greater productivity, flexibility, and even mass customization, with variations depending on the country, industry, and company context.[7] Despite having developed some key laws and regulations, the approaches and specifics of these laws vary significantly between Indonesia and South Korea.

With its growing digital economy, Indonesia has been working on strengthening its data protection framework. The Indonesian government introduced the

---

1 Asharul Islam Khan & Ali Al-Badi, "Emerging Data Sources in Decision Making and AI" (2020) 177 Procedia Computer Science at 319.

2 *Harnessing the Digital Economy for Developing Countries*, by Carl Dahlman, Sam Mealy & Martin Wermelinger (OECD Development Centre, 2016) at 17.

3 Fady A Harfoush, "Data Ethics: Facts and Fiction" in Fady A Harfoush, ed, *From Big Data to Intelligent Data: An Applied Perspective* (Cham: Springer International Publishing, 2021) at 97-98.

4 Kai Li et al, "How Should We Understand the Digital Economy in Asia? Critical Assessment and Research Agenda" (2020) 44 Electronic Commerce Research and Applications at 7.

5 Peter P Groumpos, "A Critical Historical and Scientific Overview of all Industrial Revolutions" (2021) 54:13 IFAC-PapersOnLine at 464-465.

6 Mochamad Denny Surindra et al, "Challenges of Implementing Industry 4.0 in Developed and Developing Countries: A Comparative Review" (2024) 4:3 Mechanical Engineering for Society and Industry at 479.

7 Giovanna Culot et al, "Behind the Definition of Industry 4.0: Analysis and Open Questions" (2020) 226 International Journal of Production Economics at 10-11.

Personal Data Protection Law, drawing inspiration from global standards such as the European Union's General Data Protection Regulation (GDPR).[8] However, the legal development of the matter has not been straightforward, due to the constantly developing digital landscape. Debates and discussions about how effective these laws are, and how they are implemented, remain relevant within the legal sphere. On the other hand, South Korea, known for its technological advancement, maintains a more established set of data protection laws. The Personal Information Protection Act (PIPA) in South Korea is often cited as a robust framework, albeit with its own unique challenges and nuances.[9]

One among many critical aspects of data protection laws is how data breaches are handled by data controllers, and how this is communicated to data owners. Data breach is considered a cybercrime wherein unauthorized access to certain data occurs,[10] which can result in unauthorized exposure of the data or even data theft.[11] This can include a range of information, from personal identification details such as social security numbers and financial details to trade secrets and even national security data.[12] The repercussions of data breaches can vary, including privacy invasions, financial loss, identity theft, and reputational damage.[13] To prepare for these threats, the legal framework governing digital technologies and data usage in Industry 4.0 must require data controllers to have a robust framework of cybersecurity measures, to ensure that these threats can be prevented. In turn, a comprehensive legal framework regarding data protection and notification can minimize risks associated with the breach.

---

8 Nanang Subekti, I Gusti Ayu Ketut Rahmi Handayani & Arief Hidayat, "Konstitusionalisme Digital di Indonesia : Mengartikulasikan Hak dan Kekuasaan dalam Masyarakat Digital" (2023) 2:1 Peradaban Journal of Law and Society at 9.

9 George Christou & Ji Soo Lee, "EU-South Korea Cooperation on Cybersecurity, Data Protection and Emerging Technologies" in Gertjan Boulet, Michael Reiterer & Ramon Pacheco Pardo, eds, *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives* (Cham: Springer International Publishing, 2022) at 51-52.

10 M A Baballe et al, "Online Attacks Types of Data Breach and Cyber-attack Prevention Methods" (2022) 2:5 Global Journal of Research in Engineering & Computer Sciences at 1057.

11 Ravi Sen & Sharad and Borle, "Estimating the Contextual Risk of Data Breach: An Empirical Approach" (2015) 32:2 Journal of Management Information Systems at 321.

12 David Baldwin, Jennifer Buckley & D Slaugh, "Insuring against Privacy Claims Following a Data Breach" (2018) 122:3 Penn State Law Review at 718.

13 Jenna Tugaoen, "Standing on the Ledge: Balancing Data Breaches in the Era of Technology" (2022) 50:1 Capital University Law Review at 27-28.

Indonesia and South Korea each have their own set of rules and timelines regarding when and how concerned parties should be notified in case of a breach. This is a key area where these two countries' laws can be dissected and compared.

Understanding these differences is not only a legal exercise; it has real-world implications. Digital service and platform providers, as data controllers who operate in both countries, must fulfill the legal compliance regarding data breach notification to ensure that data owners are not exposed to further risks. Moreover, with the increasing interconnectivity of the global economy, understanding these differences is crucial for international cooperation in data protection. Insights into legal cultures, priorities, and even possible future trends in data protection laws in the Asia-Pacific region can be identified by studying how Indonesia and South Korea handle data breach notifications. In turn, these insights can be used for the development of literature regarding data protection, which is crucial for legal progress today. Furthermore, this discourse is also important for understanding the importance of responsible data management, with the protection of data owner rights at the center.

The gravity of data breaches has been analyzed many times in the literature. A contextual analysis regarding this issue exists in a study conducted by Sen and Borle. This study highlights the multidimensional impacts that a data breach can have on governmental and nongovernmental sectors across different industries.[14] A counterintuitive finding of this study is the empirical evidence suggesting that investments in IT security correlate with higher risks of possible data breaches. However, the study only provides a theoretical explanation for this, detailing that organizations might have invested in an inefficient way, causing the investment costs to inflate while the risks of data breaches keep rising. The complexity and the contradictory findings of this study show that data breach in the world of cybersecurity remains an exceptionally complex issue. This conclusion is also highlighted by another study conducted by Romanosky et al., which analyzes litigations regarding data breaches.[15] The study particularly focuses on the results of litigation, which show varied percentages of settlements across different

[14] Ravi Sen and Sharad Borle, *supra note 11*.

[15] Sasha Romanosky, David Hoffman & Alessandro Acquisti, "Empirical Analysis of Data Breach Litigation" (2014) 11:1 Journal of Empirical Legal Studies at 99.

sectors. This finding further adds to the complexity of data breach legal issues by showing that different legal implications present challenges, despite cases being based on the same legal issue.

When it comes to personal data protection, the European Union's General Data Protection Regulation (GDPR) is often cited as the gold standard, as detailed by a study conducted by Mantelero.[16] The study also explained that one of GDPR's strengths is its detailed guidelines, which directly govern many processes of data management and related activities. In Sholikhah et al.'s comparative study of the legal framework for data protection in Indonesia, Malaysia, and the United Kingdom, Indonesia's legal framework is highlighted as lagging in many aspects of data protection. This is particularly due to their lack of an integrated legal framework for data protection.[17] This conclusion is outdated, due to the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law). However, the findings on the aspects that Indonesia must adequately support are still very much relevant. Additionally, whether this law can be considered an integrated and comprehensive legal framework must still be normatively evaluated. The same model of research, involving a comparative approach for normative analysis, is needed to further expand the literature regarding this topic.

A significant research gap is found in the fact that there is no development in the literature regarding the suitability of Indonesia's legal framework for addressing data breaches. This framework particularly addresses data breach notification protocols, which are important to minimize further risks associated with the data breach. To add depth to the analysis, a comparative breakdown is needed regarding the literature on Indonesia's legal framework for data protection and data breach notification protocols. To fill the analysis gap, this research utilizes the development of the same issue within South Korea's legislation and the European Union's GDPR as comparisons. As the GDPR is considered the gold

---

16 Alessandro Mantelero, "The Future of Data Protection: Gold Standard vs. Global Standard" (2020) 40 Computer Law & Security Review at 4.

17 Vina Himmatus Sholikhah, Noering Ratu Fatheha Fauziah Sejati & Diyanah Shabitah, "Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia" Indonesian Scholars Scientific Summit Taiwan Proceeding at 62.

standard of data protection, it will be used to assess whether both countries' legal frameworks for data breach measure up.[18]

II. METHODOLOGY

This research adopts a normative legal research methodology, primarily focusing on scrutinizing the distinctive legal frameworks of Indonesia and South Korea. A main focus of normative legal research is analysis of the existing legal norms within the relevant laws and regulations.[19] Normative legal research, in its pure form, typically starts with the identification of the problem. Then, it proceeds to analyze the existing norms from primary law sources to uncover the legal perspectives that govern them, as well as how they affect the problems being examined.[20] Utilizing a comparative approach, the study examines primary law sources from both countries to assess their respective data breach notification protocols. By analyzing key legislative provisions, regulations, and relevant legal precedents, the research aims to provide an in-depth understanding of the similarities and differences in how Indonesia and South Korea address data breaches and mandate notification procedures. This comparative analysis serves to identify strengths, weaknesses, and potential areas for improvement within each jurisdiction's legal framework, ultimately contributing to the enhancement of data protection practices and policies on a regional and international scale. Secondary data used in this research are primary legal sources from Indonesia and South Korea. Legal sources from Indonesia are the Undang-Undang Dasar 1945 (1945 Constitution) and Law No. 27 of 2022 on Personal Data Protection. Legal sources from South Korea are the Personal Information Protection Act, Enforcement Decree of The Personal Information Act, and General Data Protection Regulation.

---

[18] Ivan Manokha, "GDPR as an Instance of Neoliberal Governmentality: a Critical Analysis of the Current 'Gold Standard' of Data Protection" (2023) 4:2 Political Anthropological Research on International Social Sciences (PARISS) at 174.

[19] Hari Sutra Disemadi, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies" (2022) 24:2 Journal of Judicial Review at 294.

[20] David Tan, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum" (2021) 8:8 Jurnal Ilmu Pengetahuan Sosial at 2467.

III. DATA BREACH, BREACH OF RIGHTS, AND THE RIGHT TO BE NOTICED

The changes brought by Industry 4.0 span across different aspects of society. The utilization of diverse forms of digital technologies in Industry 4.0 relies heavily on data, which has become an important commodity to interconnect devices and environments.[21] Data has become so valuable that researchers have referred to its potential as the "new oil," an expression first coined in 2006 by Clive Humby.[22] Data acts as the fuel for many digital technologies, allowing them to connect and understand the needs of their users by providing the necessary user information to be analyzed by digital technology providers.

The importance of data is especially high regarding the utilization of "Big Data" and "Internet of Things" (IoT), both of which are central components of Industry 4.0 and the development of many innovations behind it.[23] The utilization of Big Data and IoT has transformed how industries operate,[24] mainly by enabling previously unattainable levels of precision, efficiency, and personalization. Their use improves many aspects of society, such as agriculture, healthcare, and transportation, bringing people closer to the realization of smart cities.[25] Through the analysis of vast amounts of data, digital platforms and services can predict consumer behavior, optimize content relevancy, and offer new products and services that meet the specific needs of their users.[26] This seamless integration and data analysis across different platforms and devices can not only enhance operational efficiencies in digital environments but also foster the creation of smart environments, from homes and offices to entire cities.

---

[21] Dr A Shaji George, "The Fourth Industrial Revolution: A Primer on Industry 4.0 and its Transformative Impact" (2024) 02:01 Partners Universal Innovative Research Publication (PUIRP) at 26.

[22] Justus Haucap, "Competition and Competition Policy in a Data-Driven Economy" (2019) 54:4 Intereconomics at 201.

[23] Xuedong Li, *Digitalizing R&D in Manufacturing Sector: Machine Learning, Infrastructure, System Architecture and Knowledge Management* Massachusetts Institute of Technology, 2021) at 15-16.

[24] Hari Sutra Disemadi, "Data Ownership in Regulating Big Data in Indonesia Through the Perspective of Intellectual Property" (2022) 13:2 Jurisdictie: Jurnal Hukum dan Syariah at 201.

[25] Ahatsham Hayat et al, "Introduction to Industry 4.0" in (Singapore: Springer Nature Singapore, 2023) at 37.

[26] Anıl Değermen & Maryam Mohammadabbasi, "Using Big Data In Analysis Of Consumer Behavior: A Qualitative Study" (2023) 12:1 KLUJFEAS at 106.

Ultimately, this can make the daily life of people more convenient, productive, and sustainable.

From a legal standpoint, these changes must be well-accommodated to ensure that the utilization of digital technologies can bring about positive changes in society, without compromising personal rights. Therefore, a legal framework must be able to address pressing concerns regarding the utilization of digital technologies, particularly regarding data protection and privacy rights.[27] There must be a sufficient standard of legal compliance that can be enforced upon digital platforms and service providers as data controllers, especially regarding privacy and the protection of data. Adequate legal compliance can ensure that data owners are protected from various dangers that can threaten their privacy rights. For this, legal compliance must contain acknowledgements and concrete protections of all rights associated with the right to privacy in the context of Industry 4.0.

Data breach is considered a cybercrime wherein unauthorized access to certain data occurs,[28] which can result in the unauthorized exposure of the data, or even data theft.[29] Breaches may include many kinds of information,[30] all of which can cause repercussions such as privacy invasions, financial loss, identity theft, and reputational damage. [31] To prepare for these threats, the legal framework governing digital technologies and data usage in Industry 4.0 must require data controllers to have a robust framework of cybersecurity measures. Such measures must ensure the prevention of these threats through a range of legal compliance that data controllers must meet, as part of their legal responsibilities in the digital space.

The legal implications of a data breach can be fundamentally interpreted as a breach of rights, underscoring legal implications between the associated risks of

---

27 Sara Quach et al, "Digital Technologies: Tensions in Privacy and Data" (2022) 50:6 J of the Acad Mark Sci at 1317-1318.

28 Muhammad Ahmad Baballe, *supra* note 10.

29 Ravi Sen and Sharad Borle, *supra* note 11.

30 David J. Baldwin, Jennifer Penberthy Buckley, and D. Ryan Slaugh, *supra* note 12.

31 Jenna Tugaoen, *supra* note 13.

digital technology's utilization and the individual's right to privacy.[32] When sensitive information is exposed without consent, it represents a violation of trust and the legal right to control one's personal information, along with a violation of business ethics.[33] This breach triggers many legal implications, including the obligation to notify affected individuals, and potentially compensation for damages. Furthermore, regulatory bodies may impose fines and sanctions to punish non-compliance with data protection laws. An example of such laws includes the GDPR in the European Union, which emphasizes the protection of personal data and privacy.[34] These legal measures are not merely punitive; they serve to reaffirm the fundamental human right to privacy, compel organizations to adopt stricter data protection measures, and ultimately sustain trust in the digital ecosystem. Through this legal lens, data breaches are not just technical failures but significant infringements on individual rights, which require a sharp legal and ethical response to prevent and mitigate their impact.

In the wake of a data breach, the right to be notified is essential within the broader individual rights of the data protection framework.[35] This right to notification is not merely a courteous gesture, but a fundamental policy embedded within the cybersecurity framework of data controllers. It acknowledges that individuals, whose personal data has been compromised, have a vested interest in being informed about such breaches promptly. Such a policy aims to empower individuals, enabling them to take appropriate measures to protect themselves against potential consequences of the breach, such as identity theft or other forms of financial and personal exploitation. The act of notification also reflects the data controller's commitment to transparency, demonstrating an understanding

---

[32] Winda Fitri, Hari Sutra Disemadi & Monica Rindiyani, "Data Leakage of Consumer Personal Data in Telecommunications Services Customer Registration: Who Is Responsible?" (2024) 4:1 Yustisia Tirtayasa : Jurnal Tugas Akhir at 100.

[33] Ewa Kulesza, "The Protection of Customer Personal Data as an Element of Entrepreneurs' Ethical Conduct" (2018) 21:7 Annales Etyka w Życiu Gospodarczym at 37.

[34] Chris Jay Hoofnagle, van der Sloot ,Bart & Frederik Zuiderveen and Borgesius, "The European Union general data protection regulation: what it is and what it means*" (2019) 28:1 Information & Communications Technology Law at 66-67.

[35] Michael Rustad & Thomas Koenig, "Towards a Global Data Privacy Standard" (2020) 71:2 Florida Law Review at 380.

that trust in their operations is contingent upon openness and honesty about security lapses.

IV. MECHANISM OF DATA BREACH NOTIFICATION IN INDONESIA VS. SOUTH KOREA

Data protection in Indonesia is mainly governed by Law No. 27 of 2022 on PDP Law. This law governs that personal data protection directs processes on and guards personal data to guarantee the constitutional rights of its subjects. The constitutional rights mentioned here stem from Article 28G paragraph (1) of the 1945 Constitution, which stipulates that every person shall have the right to protection of his/herself, family, honor, dignity, and property. It additionally states that all shall have the right to feel secure against, and receive protection from, the threat of fear to do or not do something that is a human right. Chiefly, this legal norm covers privacy rights with the right to secrecy as its aim of protection.[36] However, this is also where privacy rights in the context of data protection expand, as data breach can increase risks of associated dangers such as identity theft,[37] fraudulent charges from unauthorized access to financial accounts,[38] and the tarnishing of personal and family reputation due to the dissemination of confidential information.[39]

Mechanism of protection is covered by the PDP Law, primarily through Article 34 to 39. Article 34 governs that a Personal Data Controller shall conduct a Personal Data Protection impact assessment in the event that the processing of personal data has a high potential risk to its subject. This article lays the foundation for high-risk data management to ensure that certain types of data processing are monitored and protected differently, suggesting the need for extra

---

[36] Samuel Christian Salim & Jeane Neltje, *Analysis of Legal Protection Towards Personal Data in E-Commerce* (Atlantis Press, 2022) at 640.

[37] Fabio Bisogni & Hadi Asghari, "More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws" (2020) 10 Journal of Information Policy at 46.

[38] Lauren M Lozada, "The (Possibly) Injured Consumer: Standing in Data Breach Litigation" (2020) 93:2 St John's Law Review at 476.

[39] Natalia Semchuk, "Protection of Personal Data in the Law of Ukraine: Current Status and Recommendations for Changes" in *Scientific Space: Integration of Traditional and Innovative Processes* (Riga: Baltija Publishing, 2023) at 467.

layers of security. However, this provision is not supported by further elaboration and actual mechanisms of impact assessment, and currently still depends on the promise of further government regulation, which has not yet been enacted. Article 35 governs that Personal Data Controller is required to safeguard the security of the personal data it processes. This involves both devising and executing technical operational measures to shield personal data from unauthorized processing activities, and assessing the security level needed for the personal data. However, due to the lack of normative construction for impact assessment mechanisms, the disconnect from Article 34 renders Article 35 not fully effective.

Furthermore, Article 36 governs that a Personal Data Controller must ensure the confidentiality of personal data during its processing. Article 37 mandates that a Personal Data Controller oversee any party involved in the processing of personal data under their jurisdiction. Additionally, Article 38 requires Personal Data Controllers to safeguard personal data against any unauthorized processing activities. Lastly, Article 39 emphasizes the obligation of the Personal Data Controller to prevent illegal access to personal data. This involves utilizing secure systems for both processing and managing personal data electronically in a manner that is reliable, secure, and compliant with legal regulations. These provisions underscore a systematic approach to data protection, demanding that Personal Data Controllers enforce confidentiality, secure data against unauthorized processing, and rigorously supervise all processing activities, all of which are vital for mitigating risks like data breaches.

In reality, the highlighted provisions cannot fully guarantee the prevention of data breaches. This is mainly due to the nature of Industry 4.0's digital realm, which is constantly evolving. This means that new loopholes in digital systems that allow individuals to access data without authorization can always emerge. Understanding this, Article 46 of Indonesia's Law No. 27 of 2022 on Personal Data Protection stipulates that in the event of a failure in personal data protection, the Personal Data Controller must notify the data subject and the authority in writing no later than 72 hours from the time the Personal Data Controller was made aware of the matter. The notification should detail the personal data involved, the occurrence and nature of the exposure, and the

measures taken to address the situation. Such notifications serve to uphold the rights of individuals by keeping them informed. They additionally reinforce the importance of prompt action and transparency on the part of data controllers in managing and mitigating the consequences of data breaches.

South Korea governs the issue of data protection through the Personal Information Protection Act (PIPA), which was first enacted in 2011[40] and has since been amended multiple times, with the latest amendment was made in 2023. Article 33 of PIPA mandates public institutions to perform privacy impact assessments for personal information files at risk of breaching data-subject privacy. These assessments aim to identify and mitigate risks, taking into account factors such as the amount of personal information processed, third-party sharing, the potential for rights violations, and risk severity. The Protection Commission is authorized to designate qualified entities to conduct these assessments and may offer feedback on the results. Public institutions are required to register personal information files under scrutiny, attaching the assessment outcomes. The Commission supports the initiative by developing assessment criteria, training specialists, and disseminating guidelines. Institutions failing to uphold standards may have their assessment designation revoked, with revocation processes including mandatory hearings. The specifics of conducting privacy impact assessments are detailed in Presidential Decrees,[41] with additional regulations for legislative, judicial, and electoral bodies. Private entities are also encouraged to undertake privacy impact assessments proactively if they manage personal information files with potential risk to data subjects.

The duty to safeguard data through various mechanisms is governed by Article 29 of PIPA, which maintains that personal information controllers must implement technical, managerial, and physical safeguards. These include creating an internal management plan and maintaining access records to protect personal information from loss, theft, disclosure, forgery, alteration, or damage. Unlike

---

[40] Rina Shahriyani Shahrullah, Jihyun Park & Irwansyah Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment" (2024) 10:1 Hasanuddin Law Review at 5.

[41] Presidential decree in the context of South Korea's data protection legal framework refers to Enforcement Decree of The Personal Information Act, which has been amended many times throughout its enforcement through various Presidential Decrees.

Indonesia, there is no disconnect between this provision and the provision regarding privacy impact assessments because PIPA is supported by Enforcement Decree of The Personal Information Act (PIPA's Enforcement Decree), which covers detailed provisions on the standards for privacy impact assessments alongside the standards for data safety. This more granular regulatory ecosystem establishes PIPA as more comprehensive than PDP Law, as it includes specific regulations that address distinct aspects at the base of data protection. It also essentially covers all aspects of Article 36 to 39 of the PDP Law, providing a more efficient normative structure.

Data breach notification is covered by Article 34, which requires personal information controllers to promptly inform data subjects about any loss, theft, or exposure of their personal data. Detailing must involve the nature of the incident, its timing and method, ways to mitigate damage risk, actions taken by the controller, and contact information for assistance. This form of support aligns with South Korea's tendency to provide greater incentives for victims of data breaches.[42] If direct notification is impractical, alternative measures may be used. Controllers must also develop and implement strategies to minimize harm from such incidents. Furthermore, they must report the breach to the Protection Commission or an appointed institution, considering the incident's specifics, to receive technical support for damage control. The specifics for notification and reporting processes are further defined by PIPA's Enforcement Decree. This provision provides a more comprehensive notification compared to Indonesia's PDP Law, namely in the details on mitigating damage risk, contacting support resources, and the contents of an enforcement decree, which detail further specifics of the breach notification.

According to Article 40 of PIPA's Enforcement Decree, upon detecting a data breach personal information controllers must immediately inform affected individuals about the breach details as outlined in Article 34(1). This notification would preferably be in writing and can follow initial emergency actions like closing the access point, assessing vulnerabilities, and removing leaked information to halt further spread and additional breaches. If the full details of

---

[42] Haksoo Ko et al, "Structure and Enforcement of Data Privacy Law in South Korea" (2017) 7:2 International Data Privacy Law at 113.

the breach are not immediately known, controllers should initially notify the data subjects of the breach occurrence and the information involved, updating them with more specifics as they are confirmed. However, the weakness of this process arises in the fact that the notification does not need to be sent in a certain timeframe, which can render the notification less effective. The purpose of a timeframe for notification is to ultimately mitigate risks associated with the data breach, before the breached data is used for activities unauthorized by the data owners. An alternative provided by South Korea also comes from the same Article of PIPA's Enforcement Decree, which adds that controllers are required to notify the individuals directly and make the breach information publicly accessible on their website for at least seven days. If the controller does not have a website, it should be prominently displayed at their workplace for the same duration.

V. COMPARISON WITH THE GDPR AS THE GOLD STANDARD FOR DATA PROTECTION

Compared to GDPR, which is widely recognized as the gold standard of data protection,[43] Article 46 of the PDP Law is lacking in many ways. Article 33 of the GDPR governs that data controllers must notify the personal data breach to the supervisory authority within 72 hours, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. This provision is also supported by a more robust provision for impact assessment in Article 35 of the GDPR, in which it provides guidelines for impact assessment. Furthermore, it also governs that notification must detail the breach's nature, including the types and number of affected data subjects and records if known. It should also provide contact information for a data protection officer or another contact for further inquiries. Additionally, the notification must outline the potential consequences of the breach and the actions the controller has or will take to address and mitigate potential impact. Furthermore, in the case of a delay, the data controller must also inform the reasons for the delay to the relevant data owners, to provide even more transparency. The GDPR also

[43] Alessandro Mantelero, *supra* note 16.

governs the responsibility of data breach notification from data processor to data controller to establish a clearer line of responsibility.

The GDPR is also more rigid when compared to South Korea's PIPA and its enforcement decree, as it requires notification within a 72-hour timeframe, while South Korea demands no such thing. The responsibility to publicize a notification on data controller's website or workplace is comparably insufficient, as it requires data owners to actively interact with data controllers. Research by Mayer et al suggests that most of the time, data owners in South Korea do not know that their data was stolen or misused, and are unfamiliar with the technicality and importance of data protection.[44] Despite the provision to report to the Protection Commission with no delay, the process of accumulating data for the report takes time. Furthermore, in the event that a delay actually occurs, data controllers in South Korea are not obliged to provide an explanation, which erodes transparency. On the other hand, more time spent before the notification may also indicate the need for a careful investigation—in particular regarding the extent, depth, and potential harms of the data breach.[45] There is also a loophole that can be abused, primarily through the provision of Article 40 paragraph (2) of PIPA's Enforcement Decree, which allows data controllers to notify data owners before even confirming the details of the data breach.

South Korea's decently robust framework for privacy impact assessment makes it more capable of measuring up with the GDPR's data breach notification provisions, as privacy impact assessments help data controllers in proactively identifying and mitigating privacy risks. This, in turn, can improve the speed and quality of data breach notification. South Korea even has an edge over the GDPR in data breach notification, specifically for its provision Article 34 paragraph (1) number 5 of PIPA, regarding data controller responsibility to provide a help desk and contact points for data subjects to report damage. The GDPR also establishes a connection between data controllers and data owners, but only for the purposes of providing more information regarding the breach to data owners.

---

[44] Peter Mayer et al, *"Now I'm a bit {angry:}" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them* (2021) at 400-401.

[45] Frederik Zuiderveen Borgesius et al, "The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects" (2023) 20:2 SCRIPTed: A Journal of Law, Technology & Society at 361.

Therefore, South Korea establishes a better connection between data controllers and data owners, which is particularly important when there is damage to be compensated or fixed, depending on the nature of the damage itself. South Korea also maintains a governing body much like the EU's European Data Protection Board (EDPB) called Personal Information Protection Commission (PIPC). This body is tasked with overseeing the issue of data breaches, along with other issues regarding data protection. The EU is more flexible regarding this aspect, as Article 55 of the GDPR allows the relevant supervisory authority for each of its members to assume this role.

VI. CONCLUSION

Ultimately, the comparison demonstrates that Indonesia's legal framework is lacking in many aspects of data protection when analyzed next to South Korea and the European Union. These limitations include a lack in privacy impact assessment and a disconnect with cybersecurity compliance. Additionally, a disconnect also exists between privacy impact assessment and data breach notification. Comparatively, data breach notification processes in Indonesia are not as comprehensive as in South Korea's legal framework for data protection and the GDPR. Perhaps the most notable weakness of Indonesia's data breach notification framework is the fact that there is no governing body that specifically oversees this issue—a gap which directly hampers prompt and effective measures to deal with data breaches. South Korea and the European Union have this covered with the PIPC and the EDPB, overseeing the issues of data protection for each jurisdiction respectively. For the EU, the governing body regarding data breach can also refer to each of its members' supervisory authority. While this study contributes to the developing literature surrounding data protection, this study only identifies normative issues of data breach notification in Indonesia and South Korea. Future research can expand upon a much-needed normative model of development for both countries—with Indonesia having a higher urgency due to its inflated normative issues.

ACKNOWLEDGMENTS

The authors would like to extend their heartfelt appreciation to the Faculty of Law, Universitas Internasional Batam (UIB), for their invaluable support in providing the essential resources and facilities required for the successful execution of this research. Furthermore, we would like to express our gratitude to the members of the Research and Community Service Institute (LPPM) at UIB, as well as the dedicated research staff, for their significant guidance and assistance throughout the course of this study.

COMPETING INTEREST

In conducting this research and preparing the article, the authors declare that there is no potential conflict of interest that could influence the objectivity and integrity of the findings presented.

REFERENCES

Baballe, M A et al, "Online Attacks Types of Data Breach and Cyber-attack Prevention Methods" (2022) 2:5 Global Journal of Research in Engineering & Computer Sciences.

Baldwin, David, Jennifer Buckley & D Slaugh, "Insuring against Privacy Claims Following a Data Breach" (2018) 122:3 Penn State Law Review.

Bisogni, Fabio & Hadi Asghari, "More Than a Suspect: An Investigation into the Connection Between Data Breaches, Identity Theft, and Data Breach Notification Laws" (2020) 10 Journal of Information Policy.

Borgesius, Frederik Zuiderveen et al, "The GDPR's Rules on Data Breaches: Analysing Their Rationales and Effects" (2023) 20:2 SCRIPTed: A Journal of Law, Technology & Society.

Christou, George & Ji Soo Lee, "EU-South Korea Cooperation on Cybersecurity, Data Protection and Emerging Technologies" in Gertjan Boulet, Michael Reiterer & Ramon Pacheco Pardo, eds, *Cybersecurity Policy in the EU and South Korea from Consultation to Action: Theoretical and Comparative Perspectives* (Cham: Springer International Publishing, 2022).

Culot, Giovanna et al, "Behind the Definition of Industry 4.0: Analysis and Open Questions" (2020) 226 International Journal of Production Economics.

Değermen, Anıl & Maryam Mohammadabbasi, "Using Big Data In Analysis Of Consumer Behavior: A Qualitative Study" (2023) 12:1 KLUJFEAS.

Disemadi, Hari Sutra, "Data Ownership in Regulating Big Data in Indonesia Through the Perspective of Intellectual Property" (2022) 13:2 Jurisdictie: Jurnal Hukum dan Syariah.

———, "Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies" (2022) 24:2 Journal of Judicial Review.

Fitri, Winda, Hari Sutra Disemadi & Monica Rindiyani, "Data Leakage of Consumer Personal Data in Telecommunications Services Customer Registration: Who Is Responsible?" (2024) 4:1 Yustisia Tirtayasa : Jurnal Tugas Akhir.

George, Dr A Shaji, "The Fourth Industrial Revolution: A Primer on Industry 4.0 and its Transformative Impact" (2024) 02:01 Partners Universal Innovative Research Publication (PUIRP).

Groumpos, Peter P, "A Critical Historical and Scientific Overview of all Industrial Revolutions" (2021) 54:13 IFAC-PapersOnLine.

Harfoush, Fady A, "Data Ethics: Facts and Fiction" in Fady A Harfoush, ed, *From Big Data to Intelligent Data: An Applied Perspective* (Cham: Springer International Publishing, 2021).

Haucap, Justus, "Competition and Competition Policy in a Data-Driven Economy" (2019) 54:4 Intereconomics.

Hayat, Ahatsham et al, "Introduction to Industry 4.0" in (Singapore: Springer Nature Singapore, 2023).

Hoofnagle, Chris Jay, van der Sloot ,Bart & Frederik Zuiderveen and Borgesius, "The European Union general data protection regulation: what it is and what it means*" (2019) 28:1 Information & Communications Technology Law.

Khan, Asharul Islam & Ali Al-Badi, "Emerging Data Sources in Decision Making and AI" (2020) 177 Procedia Computer Science.

Ko, Haksoo et al, "Structure and Enforcement of Data Privacy Law in South Korea" (2017) 7:2 International Data Privacy Law.

Kulesza, Ewa, "The Protection of Customer Personal Data as an Element of Entrepreneurs' Ethical Conduct" (2018) 21:7 Annales Etyka w Życiu Gospodarczym.

Lauren M Lozada, "The (Possibly) Injured Consumer: Standing in Data Breach Litigation" (2020) 93:2 St John's Law Review.

Li, Kai et al, "How Should We Understand the Digital Economy in Asia? Critical Assessment and Research Agenda" (2020) 44 Electronic Commerce Research and Applications.

Li, Xuedong, *Digitalizing R&D in Manufacturing Sector: Machine Learning, Infrastructure, System Architecture and Knowledge Management* Massachusetts Institute of Technology, 2021).

Manokha, Ivan, "GDPR as an Instance of Neoliberal Governmentality: a Critical Analysis of the Current 'Gold Standard' of Data Protection" (2023) 4:2 Political Anthropological Research on International Social Sciences (PARISS).

Mantelero, Alessandro, "The Future of Data Protection: Gold Standard vs. Global Standard" (2020) 40 Computer Law & Security Review.

Quach, Sara et al, "Digital Technologies: Tensions in Privacy and Data" (2022) 50:6 J of the Acad Mark Sci.

Romanosky, Sasha, David Hoffman & Alessandro Acquisti, "Empirical Analysis of Data Breach Litigation" (2014) 11:1 Journal of Empirical Legal Studies.

Rustad, Michael & Thomas Koenig, "Towards a Global Data Privacy Standard" (2020) 71:2 Florida Law Review.

Semchuk, Natalia, "Protection of Personal Data in the Law of Ukraine: Current Status and Recommendations for Changes" in *Scientific Space: Integration of Traditional and Innovative Processes* (Riga: Baltija Publishing, 2023).

Sen, Ravi & Sharad and Borle, "Estimating the Contextual Risk of Data Breach: An Empirical Approach" (2015) 32:2 Journal of Management Information Systems.

Shahrullah, Rina Shahriyani, Jihyun Park & Irwansyah Irwansyah, "Examining Personal Data Protection Law of Indonesia and South Korea: The Privacy Rights Fulfilment" (2024) 10:1 Hasanuddin Law Review.

Sholikhah, Vina Himmatus, Noering Ratu Fatheha Fauziah Sejati & Diyanah Shabitah, "Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia" Indonesian Scholars Scientific Summit Taiwan Proceeding.

Subekti, Nanang, I Gusti Ayu Ketut Rahmi Handayani & Arief Hidayat, "Konstitusionalisme Digital di Indonesia : Mengartikulasikan Hak dan

Kekuasaan dalam Masyarakat Digital" (2023) 2:1 Peradaban Journal of Law and Society.

Surindra, Mochamad Denny et al, "Challenges of Implementing Industry 4.0 in Developed and Developing Countries: A Comparative Review" (2024) 4:3 Mechanical Engineering for Society and Industry.

Tan, David, "Metode Penelitian Hukum: Mengupas Dan Mengulas Metodologi Dalam Menyelenggarakan Penelitian Hukum" (2021) 8:8 Jurnal Ilmu Pengetahuan Sosial.

Tugaoen, Jenna, "Standing on the Ledge: Balancing Data Breaches in the Era of Technology" (2022) 50:1 Capital University Law Review.

Dahlman, Carl, Sam Mealy & Martin Wermelinger, *Harnessing the Digital Economy for Developing Countries*, by Carl Dahlman, Sam Mealy & Martin Wermelinger (OECD Development Centre, 2016).

Mayer, Peter et al, *"Now I'm a bit {angry:}" Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them* (2021).

Salim, Samuel Christian & Jeane Neltje, *Analysis of Legal Protection Towards Personal Data in E-Commerce* (Atlantis Press, 2022).