Journal of Central Banking Law and Institutions, Vol. 3 No. 3, 2024, pp. 547 - 584
e-ISSN: 2809-9885 – p-ISSN: 2827-7775
http://doi.org/10.21098/jcli.v3i3.271

MANAGING INDONESIAN DATA BREACH NOTIFICATION IN THE FINANCIAL SERVICES SECTOR: A CASE FOR ONE-STOP NOTIFICATION MODEL

Muhammad Deckri Algamar,[a] Abu Bakar Munir,[b] Hendro[c]
[a] Universitas Indonesia, Indonesia, [b] University of Malaya, Malaysia, [c] Deloitte, Indonesia
e-mail: deckrialgamar@gmail.com (corresponding author); abmunir@um.edu.my; hhendro@deloitte.com

Submitted: 7 February 2024 – Last revised: 23 June 2024 – Accepted: 3 September 2024

Abstract

As a business of trust, the banking and financial services industry must protect its reputation to ensure consumer's confidence. However, recent adoption of emerging internet communication technologies (ICT) have introduced new risks and challenges, such as safeguarding systems from cyberattacks and protecting consumer's personal data. Cyberattacks, especially ransomware have shed new light on the importance of privacy and security throughout the banking and financial industry's digitization efforts. Any organisation affected by cybersecurity attacks must face a twofold legal question. First, whether or not there has been a violation of the legal security requirements? Second, is to determine whether the attack triggers Data Breach Notification to the Data Protection Authority and/or Data Owners. This paper examines the complexity of maintaining security obligations under Indonesian Law (UU ITE, UU PDP, RPP PDP, and other relevant regulations) while also highlighting the common challenges in steering Data Breach Notification, with an enhanced perspective of the European General Data Protection Regulation (EU GDPR) practices. To address the challenges of patchwork data breach notification requirements in Indonesia, this paper proposes a proactive approach by Indonesia's future Personal Data Protection Authority in creating a one-stop notification model to enable effective data breach incident management and notification.

Keywords: *data breach notification, cybersecurity, personal data protection authority, financial service*

I. DATA BREACH NOTIFICATION AS KEY PRINCIPLE OF PERSONAL DATA PROCESSING IN INDONESIA

A global personal data protection legal framework is based on data processing principles to ensure that normative requirements of the law can go hand-in-hand with the foundational principle throughout personal data processing. The historical roots of these principles can be traced to OECD Principle 1980 and Council of Europe 108+ Convention that sets out the early framework of personal data processing principles; this framework has then been modernised

and adapted into various jurisdictions around the world.[1] Most notably, the European General Data Protection Regulation (the "EU GDPR") became the most comprehensive and mature data protection framework that first adopted personal data processing principles. However, the norms under the EU GDPR have continued to influence and inspire other countries beyond EU Member States' jurisdiction in drafting their national privacy laws.[2] In 2021, Graham Greenleaf pointed out that the EU GDPR as a data protection legal framework has become a major inspiration for over 145 data protection laws across the globe.[3] This includes Indonesia's recently enacted Law No. 27 Year 2022 on Personal Data Protection ("UU PDP") that contains similar data processing

Table 1.
Data Processing Principles under UU PDP & EU GDPR

No.	UU PDP Principles	EU GDPR Principles
1.	Personal Data collection must be conducted in a limited manner, specific, lawful, and transparent	"Lawfulness, fairness, and transparency"
2.	Personal Data processing must be conducted in accordance with its purpose	"Purpose limitation"
3.	Personal Data processing is conducted by ensuring the rights of Personal Data Subject	No similar principle is found
4.	Personal Data processing must be conducted accurately, complete, not misleading, up-to-date, and in accountable manner	"accuracy"
5.	Personal Data processing is conducted by protecting the security of Personal Data from unauthorised access, unauthorised disclosure, unauthorised alteration, misuse, destruction, and/or loss of personal data	"Integrity and confidentiality"
6.	Personal Data Processing is conducted by informing the purpose and processing activity in addition to failure of Personal Data Protection	No similar principle is found
7.	Personal Data shall be destroyed and/or deleted after the retention period expires, or at the request of Personal Data Subject, unless otherwise stipulated by laws and regulations	"Storage limitation"
8.	Personal Data processing is conducted responsibility and can be clearly proven	"accountability"

[1] Dara Hallinan and Frederik Zuiderveen Borgesius, "Opinions Can Be Incorrect (in our opinion!) On Data Protection Law's Accuracy Principle," *International Data Privacy Law*, 10, no. 1 (2020): 2.

[2] R. O Brien, "Privacy and security: The new European data protection regulation and it's data breach notification requirements," *Business Information Review,* 30 (2016): 81.

[3] Graham Greenleaf, "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance," 169 Privacy Laws and Business International Report, 1, (2021): 3-5.

principles throughout data collection, data usage, data storage, data transfer, and data erasure to any entities processing Personal Data. The similarities are illustrated in the table below:[4]

Although data processing principles related to "data minimization" or "lawfulness, fairness, and transparency" are commonly found both under UU PDP and the EU GDPR, Indonesia uniquely introduced a new principle that essentially mandates that "Personal Data Processing is conducted by informing the purpose and processing activity in addition to failure of Personal Data protection."[5] This new principle encapsulates two aspects: first, is the requirement to inform data subjects on the purpose and name of processing activity, which coincides with other data processing principles under UU PDP.[6] The second aspect becomes the foundational principles in delivering Data Breach Notification, a key aspect of cybersecurity incident response management. Further technical application of the latter is found under the current Draft Government Regulation on Implementation of PDP Law ("RPP PDP"), where the current draft expands the principle through implementing a lawful Data Breach Notification system, establishing and implementing policies/procedures/guidelines to prevent and mitigate cyber incidents.[7] This emphasis on Data Breach Notification is both found as principle (Article 16 UU PDP) and a separate requirement (Article 46, UU PDP), making Indonesia the only jurisdiction in the world to encapsulate Data Breach Notification both as a data processing principle and key privacy obligation.

The legal framework of Personal Data Protection is not limited to UU PDP, a sector specific requirement must also be taken into account for compliance with privacy regulations in Indonesia. For instance, in the financial sector, the newly enacted Bank Indonesia Governor Board Member Regulation No. 20 Year 2023 on the Implementation of Consumer Protection ("PADG 20/2023") recognizes the importance of Personal Data Protection as part of key principle in consumer protection.[8] Specifically, PADG 20/2023 elucidates that payment systems and services operators must always maintain confidentiality and security of data and/or consumer information by using data in accordance

---

4 Indonesia, *Personal Data Protection Law*," Law No. 27 of 2022, Article 16 Section (2).

5 Indonesia, "*Personal Data Protection Law*," Article 16 Paragraph (2) Point f.

6 Indonesia, "*Personal Data Protection Law*," Article 16 Paragraph (2) Point a and b.

7 Indonesia, "*Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law*, Article 30 Point d, e, and f.

8 Bank Indonesia, "*Amendment of Regulation of the Members of the Board of Governors*," Regulation No. 20 of 2023 on the Implementation Procedure of Consumer Protection of Bank Indonesia, Article 3 Paragraph 1 Point f.

with the interests and purposes that have been consented to by consumers.[9] PADG 20/2023 is amongst the new series of privacy regulation introduced in the financial sector, with other regulation such as SEOJK 29/2022 on Cybersecurity and Resilience in addition to PBI 23/6/PBI/2021 on Payment Services Providers that mandates a reliable and safe cybersecurity system. Additionally, the importance of several financial institutions might result in the applicability of privacy and security requirements under Presidential Regulation No. 82 Year 2022 on Vital Information Infrastructure if the financial company's electronic system is categorised under critical infrastructure.[10]

Within the aforementioned context, it is imperative for any companies in the financial services industry to adapt to the new wave of privacy regulations, not only to comply with the minimum requirements, but also build trust with consumers in the area of cybersecurity. However, the amount of sensitive data, including personal financial information, makes this industry the most susceptible to cyberattacks that are profit-oriented, including Ransomware attacks on several major banks and financial services institutions globally.[11] Unfortunately, many companies prior to UU PDP have silently gotten away with concealing cyber incidents without having to deal with any legal repercussions in maintaining a secure system or providing Data Breach Notifications as part of transparency obligations.[12]

Previous writings on the legal liability for failure to notify of data breaches[13] and calls to establish a Data Protection Authority[14] has been extensively discussed under the regime of Law No. 11 of 2008 on Electronic Information and Transactions ("UU ITE") supported by Government Regulation No. 71 Year 2019 on Electronic System Provider ("PP 71/2019") and Ministry of Communication and Information Regulation No. 20 Year 2016 ("Permenkominfo 20/2016"). However, there is now a greater need to understand privacy and security requirements under UU PDP alongside

[9] Bank Indonesia, "*Amendment of Regulation of the Members of the Board of Governors*," Regulation No. 20 of 2023 on the Implementation Procedure of Consumer Protection of Bank Indonesia, **Elucidation of** Article 3 Paragraph 1 Point f.

[10] Indonesia, "*Presidential Regulation on Protection of Vital Information Infrastructure*," Regulation No. 82 of 2022, Article 13.

[11] Abdulbasit Darem, et.al., "Cyber threats classifications and countermeasures in banking and financial sector," IEEE Access, Vol 11 (2023): 125139.

[12] Edmon Makarim, "The Law Against Personal Data Leaks," *Public Relation of Faculty of Law Universitas Indonesia,* July 10, 2020, https://law.ui.ac.id/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh-edmon-makarim/.

[13] Maichle Delpiero, et al., "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban *Online Marketplace* dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data." *Padjadjaran Law Review*, 9, no. 1 (2021): 13-16.

[14] Gunardi Lie, Dylan Aldianza Ramadhan, and Ahmad Redi, "Independent Commission of Personal Data Protection: Quasi-Judicial and Efforts to Create Right to be Forgotten in Indonesia," *Jurnal Yudisial*, 15, no. 2 (2022): 241-243.

its intersection with sectoral regulations, when security failures arise, and the triggering events for Data Breach Notification especially in the financial sector, which processes high volumes of sensitive Personal Data. In turn, this paper also explores the practical issue of Data Breach Notification in Indonesia by comparing Indonesia's legal framework with Data Protection Authorities across European Union *(Datatilsynet, Tietosuojavaltuutetun toimisto, Gegevensbeschermingsautoriteit,* the Irish Data Protection Commission, and the Cyprus Data Protection Commission). Thus, this paper explores two legal questions:

1. How does Indonesia and the EU set out security requirements for Personal Data Protection in the financial sector?
2. How does Indonesia and the EU determine Data Breach Notification triggers, notification procedures, and the involvement of the Personal Data Protection Supervisory Authority?

In order to answer these questions, this paper is divided into four sections. First, the introduction to principles and legal framework of cybersecurity and data protection as mentioned above. Second, a discussion of the cyber risk landscape in the financial sector with a focus on Ransomware as an emerging cybersecurity threat. Third, an analysis of cybersecurity and data protection requirements that must be considered in response to a cyber incident, followed by an analysis of Data Breach Notification triggers to Data Subjects and/or Data Protection Supervisory Authorities. Lastly, we propose a One-Stop Notification Model to mitigate the existing cumbersome and fragmented procedures, with the aim of streamlining cyber incident management for Data Controllers, especially in the financial services sector where it must currently notify multiple supervisory authorities.

II. CYBER RISK LANDSCAPE OF THE FINANCIAL SECTOR: A STUDY ON RANSOMWARE ATTACKS

In the realm of cyber risk, there are three categories of cyber incidents that must be mitigated: (i) incidents due to malicious actors; (ii) incidents due to failure of an organisation's systems; and (iii) incidents due to human error.[15] Out of all three, the first category is the most severe due to possible follow-up actions by malicious actors based on financial incentives that could harm Data Subjects directly.[16] This is clearly exemplified in one of Indonesia's

[15] Eleni Kosta, "Thematic Document: Security of Processing and Data Breach Notification," *European Data Protection Board* (November 2023): 8.

[16] "NCCA Hearing Meeting with Commission I The House of Representatives of the Republic of Indonesia," National Cyber and Crypto Agency, accessed 8 February 2024, https://www.bssn.go.id/rapat-dengar-pendapat-bssn-bersama-komisi-i-dpr/.

biggest Sharia Bank incidents in May 2023, where a Ransomware group called Lockbit 3.0 attacked the institution. In this case, the bank first experienced a complete system failure on 8 May 2023, where customers could not access their bank services at all, this included preventing customers from conducting transactions, paying bills, or even taking monthly payroll. In response to this, the bank stated that maintenance was being conducted with no confirmed cyber incidents despite suspicion from the public.[17] As customers remain anxious, LockBit 3.0 publicly announced that a cyber-attack had been deployed against the Sharia Bank after installing Ransomware that encrypted more than 1.5 terabytes of data containing more than 15.000 customers' personal data. LockBit 3.0 threatened to release the data to the public if the Sharia Bank failed to pay a ransom of $200.000.000 within 72 hours.[18] After receiving the news, the Sharia Bank only recognized this Ransomware attack from the malicious group as a generic, one-line *"serangan siber"* in its 11 May 2023 press statement.[19]As customers scrambled in fear of their safety, the Sharia Bank's continued statements guaranteeing their customer personal data had become empty promises after LockBit 3.0 leaked all of their ransomed data into the Dark Web after failed negotiations.[20]

The LockBit 3.0 attack is part of the emerging trend of Ransomware attacks against financial institutions. Ransomware is software that is specifically designed to lock its victims' systems through forced encryption, enabling only the hackers to have access to the data, which can include photos, personal data, confidential information, or databases of its targets. Public institutions, businesses, and even individuals have been victimised by Ransomware. As a business model, Ransomware organisations use an aggressive tactic to extort their victims after taking control of corporate or institutional assets, and promises to provide encryption keys and leave the information intact if the victims are willing to pay a ransom.[21] Ransomware organisations also

[17] "PRESS RELEASE BSI President Director: We Apologize and Are Trying to Restore Services," Bank Syariah Indonesia, accessed 8 February 2024, https://ir.bankbsi.co.id/newsroom/dc70693fac_d7743dac9a.pdf.

[18] "LockBit hackers pocket 15 million BSI customer records, threaten to sell them if negotiations fail," Merdeka.com, accessed 8 February 2024, https://www.merdeka.com/teknologi/hacker-lockbit-kantongi-15-juta-data-nasabah-bsi-ancam-dijual-jika-negosiasi-gagal.html.

[19] "PRESS RELEASE BSI Branch, ATM & Mobile Banking Services Have Returned to Normal," Bank Syariah Indonesia, accessed 8 February 2024, https://ir.bankbsi.co.id/newsroom/1a92cc8ca2_4364ce956d.pdf.

[20] Erwin Pratama, "Negotiation period ends, LockBit reveals BSI data on the Dark Web," Tempo.co, accessed 8 February 2024, https://tekno.tempo.co/read/1726219/masa-negosiasi-berakhir-lockbit-ungkap-data-bsi-di-dark-web.

[21] Stuard E. Madnick, "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase," *Apple*, December 2023, 11, https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.

target organisations by utilising Ransomware-as-a-services method, where it persuade and recruits individual outside the Ransomware group (such as former employees, insiders, or unassociated hackers) to implant Ransomware in the target's system and share profit after a successful attack.[22] LockBit 3.0 is among the most successful Ransomware groups to operate by strategically targeting organisations with valuable information such as Personal Data or classified information to be used as leverage during ransom negotiations.

This method of cyberattack has skyrocketed since COVID-19 after mass digitization efforts by many organisations that are not backed by proper cybersecurity and data governance, especially in the banking industry. Badan Siber dan Sandi Negara ("BSSN") has reported more than 160.000.000 malware anomalies in Indonesia, making it among the highest number of cyberattack categories in the region.[23] With enhanced capabilities, there is an expected surge of Ransomware-based cyber-attacks in the near future.[24] A similar number of Ransomware attacks is also reflected in various jurisdictions, with Ransomware rising to become the most lucrative malware attacks with predicted global damages exceeding $20 trillion annually by 2031.[25]

After being aware of the Ransomware attack, a victim must balance whether or not to pay the ransom. While it remains one of the most difficult question to answer, statistically, 83% of Ransomware attacks globally were paid by organisations because it is believed that it is the quickest and easiest route to ensure business continuity and also to prevent the retrieved consumers' personal data from being leaked for failure to pay.[26] In conjunction with this, Ransomware groups have played their interpretation of data protection laws against their victims. For instance, they claim the ransom payment would be

---

[22] "The Prolificacy of LockBit Ransomware," The Hacker News, accessed 8 February 2024, https://thehackernews.com/2023/03/the-prolificacy-of-lockbit-ransomware.html.
Mourad Benmalek, "Ransomware on Cyber-Physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges," *Internet of Things and Cyber-Physical Systems* 4 (2024), 193. https://doi.org/10.1016/j.iotcps.2023.12.001.

[23] Agustinus Rangga Respati, Aprillia Ika, "NCCA Mentions the Potential for Cyber Attacks is Still High, Especially the "Ransomware Type" Kompas.com, accessed 8 February 2024, https://money.kompas.com/read/2023/11/15/114406526/bssn-sebut-potensi-serangan-siber-masih-tinggi-terutama-jenis-ransomware.

[24] "Dark Web Profile: LockBit 3.0 Ransomware," SOCRadar, accessed 8 February 2024, https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/#:~:text=LockBit%203.0%20is%20a%20Ransomware,businesses%20and%20critical%20infrastructure%20organizations.

[25] Benmalek, "Ransomware on Cyber-Physical Systems: Taxonomies, Case Studies, Security Gaps, and Open Challenges," *Journal Internet of Things and Cyber-Physical Systems 4* (January 2024): 186.

[26] "83% of organizations paid up in ransomware attacks," VentureBeat, accessed 8 February 2024, https://venturebeat.com/security/83-of-organizations-paid-up-in-ransomware-attacks/.

cheaper compared to full-on financial penalty by data protection authorities.[27] As a consequence, many companies are persuaded by the Ransomware organisation, seeing it as the best solution to settle the incident as quickly and discreetly as possible.

This interpretation is incorrect, however, as whether the ransom is paid or not does not ameliorate a company's failure of its data protection obligations.[28] Nadir and Bakhshi argued that any form of payment to attackers is not ideal for three reasons. First, complying with Ransomware demands would reward the business model operated by Ransomware groups and provide greater incentive and resources to enable future attacks, thus denying payment would be the first step in stopping the Ransomware industry. Second, there are no guarantees of the encryption key actually working as seen in several WannaCry Ransomware attacks. In addition, it is also possible for the attackers to request more money after initial payment was made. Third, ransom payments do not guarantee any more attacks as the hackers already know the vulnerabilities to be exploited at a later stage.[29] In fact, there are trends for malicious hackers threatening to sell important files or data to competitors for them to exploit.[30] However, despite all the reasons to not pay ransom, the time-sensitive nature and operational pressures of Ransomware attacks might persuade the organisation to pay, as the majority does.

In paying ransoms for cyberattacks, negotiation is a key part in managing Ransomware attacks. Like its name, hacker groups will set up a price that must be paid as a ransom, paying will provide victims with the needed encryption key to ensure no further harm is done, while failure to pay often leads to data leaks and other malicious actions from the hackers.[31] In its analysis on the dynamics of Ransomware negotiation, Ryan et al. describe that attackers refuse to counter with a lower offer because of several factors,[32] First, Ransomware groups need to maintain their status as a threat, and willingness to accept counter offers will demonstrate weakness and trend of accepting lower counteroffers. Two, while a quick negotiation is desirable, attackers do not lose

[27] Anne Gotay, How Ransomware Shakes Up GDPR Compliance, Sotero, accessed 8 February 2024, https://www.soterosoft.com/blog/how-ransomware-shakes-up-gdpr-compliance/.

[28] Marianne Kolbasuk McGee, "Irish Authorities Levy GDPR Fine in Centric Health Breach," Bank Info Security, accessed 8 February 2024, https://www.bankinfosecurity.com/irish-authorities-levy-gdpr-fine-in-centric-health-breach-a-21346.

[29] Ibrahim Nadir and Taimur Bakshi, "Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques," *International Conference on Computing, Mathematics and Engineering Technologies* (2018): 5.

[30] Tom Meurs, et al., "Deception in Double Extortion Ransomware Attacks: An Analysis on Profitability and Credibility," *Computers & Security* 138, (2024): 3.

[31] Pierce Ryan, et. al., "Dynamics of Targeted Ransomware Negotiation," *IEEE Access*, 10 (2022): 32839.

[32] Pierce, "Dynamics," 32839.

out in the prolonged negotiation, whereas victims may lose more money and reputation as a consequence of prolonged Ransomware disruption. Therefore, it is quite clear that Ransomware attackers are not persuaded by sudden lower offers from its victims to the contrary, it might act more aggressively to the victims.

Ransomware and other cyber-attacks against financial institutions will be on the rise, as these types of businesses hold valuable personal data which includes financial records, account numbers, and even access to customer credentials that can be lucrative for hackers to exploit as part of an attack. To exemplify this, the Central Bank of Indonesia itself was allegedly attacked by another Ransomware group in 2022 that targeted non-critical employee data,[33] and a financial lending institution was also attacked in May 2023 by unconfirmed malware which led to an operational switch off during the incident. [34] Thus, there is a strong urgency to emphasise the protection of Personal Data in the banking and financial services institutions to prevent attacks from opportunistic hackers.

III. NAVIGATING CYBSERCURITY AND MANDATORY DATA BREACH NOTIFICATION REQUIREMENTS

After understanding the background of Ransomware as a cybersecurity threat, it is important to recognize the legal requirements set out within Indonesia. In principle, Indonesia's legal regime for information privacy and data security stems from UU ITE that was enacted in 2008. Article 16 of UU ITE requires that every electronic system provider protect the availability, integrity, authenticity, confidentiality, and availability of electronic systems throughout their operations, thus providing the first requirement of cybersecurity to protect all electronic information (regardless whether the information contains Personal Data or not).[35] While UU ITE provides a security requirement, it is also the first law that prohibits IT-based crimes such as illegal access, cracking, and hacking which entails legal repercussions for malicious actors.[36] In 2022, the

[33] "Expert Calls Conti Ransomware Gang that Breached BI Dangerous Hackers," CNN Indonesia, accessed 8 February 2024, https://www.cnnindonesia.com/teknologi/20220120191930-185-749298/ahli-sebut-geng-ransomware-conti-yang-bobol-bi-peretas-berbahaya.

[34] Yunia Rusmalina, "Not Ransomware, BFI Finance Admits to Malware Attack," Bloomberg Technoz, accessed 8 February 2024, https://www.bloombergtechnoz.com/detail-news/7300/bukan-ransomware-bfi-finance-akui-terkena-serangan-malware.

[35] Indonesia, "*Electronic Information and Transactions Law*," Law No. 11 of 2008, Article 16.

[36] Mochammad Tanzil Multazam and Noor Fatimah Mediawati, "Personal Data Collection: Recent Developments in Indonesia," *2nd Virtual Conference on Social Science in Law, Political Issue and Economic Development* (2022): 52.

most recent development was found under UU PDP that specifically regulates the protection of Personal Data, where every entity that processes Personal Data must ensure no failure of Personal Data, including failure to maintain confidentiality, integrity, or the availability of Personal Data. In the context of cyber incidents such as Ransomware attacks, there are two requirements that must be considered: first is to determine whether a security measure is adequate, and second is to determine whether a Data Breach Notification is required as discussed in the following sub-section.

III.A. Legal Framework for Cybersecurity Requirements in Indonesia and European Union

UU PDP established a twofold security scheme. First is through the mandatory adherence with "security principles" mentioned in Section I as Personal Data processing must be carried out by protecting it from unauthorised access, unauthorised disclosure, unauthorised alteration, misuse, and accidental destruction and/or loss of Personal Data.[37] This principle is further elaborated in the RPP PDP,[38] while future changes are expected from the current draft, the following measures can be utilised as guiding actions in preparing compliance to the "security principle:[39]

a. Establishing security measures to limit authority for accessing, rectifying, disclosing, and deleting personal data; ensuring accuracy of storage and processing; preparing recovery measures if a data is accidentally lost, altered, or destroyed;
b. Conducting risk analysis on personal data processing activities to determine the appropriate level of security measures;
c. Establishing information security and personal data protection policy while ensuring the appropriate steps in implementing the policies;
d. Periodically reviewing the information security and personal data protection policy;
e. Establishing basic technical control;
f. Implementing Personal data protection mechanism through encryption and/or masking;

---

[37] Indonesia, "*Personal Data Protection Law*," Law No. 27 of 2022, Article 16 Paragraph (2) Point e.

[38] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law*, Article 29.

[39] "Press Release No. 256/HM/KOMINFO/08/2023 Drafting Implementing Rules, Kominfo Opens Public Participation Through the pdp.id," Public Relations Bureau of the Ministry of Communication and Information, accessed 8 February 2024, https://www.kominfo.go.id/content/detail/51157/siaran-pers-no-256hmkominfo082023-tentang-susun-aturan-pelaksana-kominfo-buka-partisipasi-publik-lewat-laman-pdpid/0/siaran_pers.

g. Discerning, determining, and implementing parameters for confidentiality, integrity, availability, authentication, wholeness, and accountability of the Personal Data processed;
h. Ensuring that access to Personal Data can be recovered in the case of cyber incidents through creating backup process in accordance with the laws and regulations; and
i. Conducting periodical testing and review against the security control procedures to ensure the activity remains effective and continuous.

As a second layer of protection, UU PDP provides three security-related requirements that must be taken during Personal Data processing. Article 35 UU PDP maintains that both the Data Controller and the Data Processor must set out technical operational measures in protecting Personal Data Security.[40] Similarly, RPP PDP has drafted the implementing steps of "technical operational measures" such as pseudonymization/encryption measures for Personal Data, ensuring the system is capable in retrieving access and returning availability in case of technical or physical incidents, and requires Data Controller or Data Processor to periodically test, evaluate, and assess the effectiveness of the aforementioned measures to ensure security of Personal Data processing.[41] The two other requirements are found under Articles 36 and 39 UU PDP that mentioned similar requirements under UU ITE, as Article 36 requires maintaining the confidentiality of Personal Data and Article 39 creates an obligation to prevent Personal data from being illegally accessed.[42] It is to be understood that the requirement to prevent illegal access remains incomplete, as Article 39 Paragraph (2) UU PDP limits the scope of this obligation only to implementing a reliable, safe, and accountable system, but is silent on whether a system is considered "reliable, safe, and accountable" when a malicious attackers, such as Ransomware organisation has successfully breached the system despite best efforts from Data Controller or Data Processor.

In comparison with EU GDPR, UU PDP provides more stringent security requirements. EU GDPR only has 1 (one) security requirements found under Article 32, which provides any Data Controller or Data Processor to "implement appropriate technical and organisational measures."[43] This can be conducted through non-exhaustive list of action such as: (i)pseudonymization and encryption; (ii) ensuring confidentiality, integrity, availability, resilience of system and services; (iii) capacity to restore availability and access to Personal Data in case of physical or technical incident; (iv) regular testing, assessing, and

[40] Indonesia, "*Personal Data Protection Law*," Law No. 27 of 2022, Article 35.

[41] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law*, Article 131 Paragraph (2).

[42] Sinta Dewi Rosadi, *Pembahasan UU Pelindungan Data Pribadi,* (Jakarta: Sinar Grafika, 2023), 102.

[43] European Union, "General Data Protection Regulation," Regulation 2016/679, Article 32.

evaluating the effectiveness of technical and organisational measures to ensure security of processing.[44] Cedric Burton in his analysis of "appropriateness" of technical and organisational measures determined that the action taken must correlate with the risk associated with Personal Data processing activities. Not all measures mentioned under Article 32 (a-d) under EU GDPR must be taken, but EU regulators have indicated a clear preference for these measures to be taken by Data Controllers or Processors.[45]

In stark contrast to Article 36 and Article 39 UU PDP, there is no obligation to maintain complete confidentiality or ensure no illegal/unauthorised access to Personal Data under EU GDPR. As a result, not every breach of a system would result in violation of security requirements under EU GDPR. Within the same line of argumentation, Advocate General Giovanni Pitruzella stated that in order to be exempted from liability on violation of Article 32 EU GDPR, Data Controller must demonstrate that it is not in any way responsible for giving rise to the event which causes damage.[46] Thus, an assessment must be made on a case-by-case basis regarding the appropriate technical or organisational measures taken by the Data Controller alongside its effectiveness by the court of the Data Protection Authority.[47]

However, as it has been made clear, no security measures can completely prevent the possibility of attack or compromise. Therefore, complying with the cybersecurity requirements does not serve as a proof there will be no cyber incident or data breach. Not every data breach is a violation of cybersecurity requirements, however the next step after realising a system has been attacked is to assess whether a data breach triggers mandatory notification.

III.B. DATA BREACH NOTIFICATION: NAVIGATING COMPLEXITY OF INFORMING CYBER INCIDENTS IN INDONESIA AND EUROPEAN UNION

After establishing and meeting the security requirements related to Personal Data, the next step any company must prepare for is an effective Data Breach Notification procedure. As mentioned previously, no security system can be completely impenetrable and thus companies need to prepare an incident response policy, which includes steps for determining when to send notifications. While companies must ensure compliance the guidelines for mitigating a data

[44] European Union, "General Data Protection Regulation," Regulation 2016/679, Article 32 Point A-D.

[45] Cedric Burton, "Article 32: Security of Processing" in Christopher Kuner the EU General Data Protection Regulation: A Commentary (Oxford: Oxford University Press, 2020), 635-636.

[46] "Advocate General Opinion in Case C-340/21, Press Release No. 67/23," Court of Justice of the European Union, accessed 8 February 2024, https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-04/cp230067en.pdf.

[47] Eleni, "Thematic," 8.

breach and recovering the system as quickly as possible, it must also take into account the obligation of drafting and sending out notifications within the stipulated timeline (72 hours or 3x24 hours) regardless of the cause of the security incident, by internal negligence or due to malicious actors externally. In Indonesia, the obligation to conduct Data Breach Notification arises when "failure of Personal Data Protection" occurs,[48] although the practice remains ambiguous as this section establishes.

A Data Breach Notification is not merely a simple statement made by the public relations division to preserve a company's reputation, privacy laws require mandatory elements that must be included in the notification to ensure the notification is lawful and provides meaningful information. In essence, there are two types of Data Breach Notifications: i) addressed to supervisory authority or authorities;[49] and ii) addressed to Data Subjects.[50] Prior to UU PDP, there had been sectoral regulations pertaining Data Breach Notification. Similarly, after UU PDP, there has also been sectoral regulations that provide different specifications for conducting the same notification with no clear delineation of which requirement takes precedence. Therefore, to formulate a comprehensive Data Breach Notification in the financial sector, there are three key regulations that need to be considered in conjunction. First, Ministry of Communication and Informatics Regulation No. 20 Year 2016 on Electronic Personal Data Protection & Government Regulation No. 71 Year 2019 on Private Electronic System Operators which governs data breach in the context of electronic system providers failure.[51] Second, Indonesia's Law No. 27 of 2022 on Personal Data Protection which regulates data breach notification procedures in the context of failure to protect Personal Data. Third, is Indonesia's Financial Services Authority Circular Letter No.29/SEOJK.03/2022 that establishes a Data Breach Notification form for incidents specifically for the financial sector. While all three regulations diverge from each other with no clear *lex specialis*, understanding the key aspects from each regulation are necessary for drafting a proper Data Breach Notification.

---

[48] Under PDP Law Article 46 (1) Explanation: "Data Protection Failure" refers to the failure of protection the confidentiality, integrity, and availability of personal data, including security violations that is intended or not intended which includes to the destruction, loss, alteration, disclosure, or unauthorised access to personal data transmitted, stored, or processed.

[49] Indonesia, "*Personal Data Protection Law*," Law No. 27 of 2022, Article 46 Paragraph (1) Point b.

[50] Indonesia, "*Personal Data Protection Law*," Law No. 27 of 2022, Article 46 Paragraph (1) Point a.

[51] Pursuant to Government Regulation No. 71/2019 on Private Electronic System Operators Article 24 Explanation, "Failure" refers to the cessation partly or wholly of Electronic System function which are essential so that the electronic system does not function properly.

First, for electronic system providers, a Data Breach Notification is triggered when a "Failure" occurs.[52] This term is elucidated under Article 24 PP PSE as "part or complete cessation of Electronic System function which are essential so that the electronic system no longer functions properly."[53] When such circumstances arises, a Data Breach Notification must be sent out to both relevant subjects and supervisory authority within 14 days after the Failure is discovered,[54] in accordance with the minimum requirement under Article 14 Paragraph (4) of PP PSE in conjunction with Article 28 of Permenkominfo 20/2016:

1. Include the reason or cause of Data Protection Failure;
2. Send to the victim or victims within a maximum of 14 days after a Data Protection Failure is discovered;
3. Ensure Data Breach Notification is directly received by the relevant victim or victims of Data Protection Failure; and
4. Received in a written format, unless consent has been established to send the Data Breach Notification electronically.

Permenkominfo 20/2016 also establishes the principle of "good faith" in sending out Data Breach Notifications.[55] While no mention of what this principle entails, it can be agreed that sending notifications in a timely manner is vital to minimising the potential impact that can occur. Furthermore, Article 28(i) of Permenkominfo 20/2016 also mandates an easily reachable contact person for data subjects to liaise with[56] This is especially important in the context of Data Breaches where Data Subjects need an emergency helpline to ensure that their information is safe or wanting to know further information specific to the subject.

Second, for Personal Data Protection, UU PDP alongside RPP PDP are relevant as they provide a different framework for Data Breach Notification. There are diverging points that sets UU PDP apart from its predecessor including: (i) trigger and content of notifications; (ii) existence of public notifications; and (iii) timeline for Data Breach Notification as explained below.

---

[52] Indonesia, "*Electronic System and Transaction Operation Regulation,*" Government Regulation No. 71 of 2019, Article 24 Paragraph 3.

[53] Indonesia, "*Electronic System and Transaction Operation Regulation,*" Government Regulation No. 71 of 2019, Elucidation of Article 24.

[54] There is no distinction between notification send to supervisory authority and data subjects under this regulation.

[55] Indonesia, "*Protection of Personal Data in Electronic Systems Law,*" Regulation of the Minister of Communication and Information Technology No. 20 of 2016, Article 2, Paragraph 2, Point f.

[56] Indonesia, "*Protection of Personal Data in Electronic Systems Law,*" Regulation of the Minister of Communication and Information Technology No. 20 of 2016, Article 28, Point i.

On the first point, a mandatory Data Breach Notification is triggered every time a "Personal Data Protection Failure" occurred,[57] unless the failure does not result in any disclosure of Personal Data.[58] Article 46 of UU PDP provides clearer guidelines on the terms, it refers to a failure of protection the confidentiality, integrity, and availability of personal data, including security violations that is intended or not intended which includes to the destruction, loss, alteration, disclosure, or unauthorised access to personal data transmitted, stored, or processed.[59] Similar to PP 71/2019 or Permenkominfo 20/2016, there is no distinction between the minimum information provided to supervisory authority or data subject. Existing draft or RPP PDP establish that Data Breach Notification must at least include:

1. Personal Data that has been compromised;
2. Chronology of (how and when) the compromise occurred;
3. Impact of the Personal Data Protection failure, followed by mitigation and recovery efforts to the compromised Personal Data; and
4. Contact of person-in-charge.

On the second point, UU PDP also maintains that a public notification must also be conducted in special circumstances. This circumstance is drafted under UU PDP where an incident has: a) disrupted public services; b) seriously affected public interest; or c) causes the impossibility for Data Controllers to ensure notification can be directly received by Data Subjects.[60] This issue is further analysed after comparison with EU GDPR at the end of this section, there is no guideline or indication to determine when a public notification is necessary and whether it erases the obligation to notify Data Subjects individually in Indonesia.

Lastly**,** UU PDP provides a significantly diverging timeline of Data Breach Notification when compared to the Electronic System Providers regime. Article 46 UU PDP determines a *prima facie* shortened timeline of 3 x 24 hours to conduct Data Breach Notification.[61] However, RPP PDP further clarifies that the clock only starts ticking after a Personal Data Protection failure is discovered with certainty, appropriately, and reasonably according to the conclusion made from the documentation process of an incident.[62] There is

---

[57] Indonesia, "*Personal Data Protection Law*," Article 46.

[58] Indonesia, "*Personal Data Protection Law*," Article 46, "*Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 124 Paragraph (5).

[59] Indonesia, "*Personal Data Protection Law*," Elucidation of Article 46.

[60] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 124 Paragraph (4).

[61] Indonesia, "*Personal Data Protection Law*," Article 46 Paragraph (1).

[62] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 124 Paragraph (2) and Elucidation.

no further guidance on the process of documentation, as Article 125 RPP only clarified the content of documentation as the following:[63]

1. Root cause of the failure;
2. Timing and chronology of the failure;
3. Affected Personal Data;
4. Consequences of the data protection failure;
5. Mitigation and recovery measures;
6. Conclusion on whether a compromise has occurred to Personal Data
7. Timeline of Data Breach Notifications addressed to Data Subject and PDP Authority; and
8. Risk of Personal Data compromise to Data Subjects.

The documentation must be delivered to the PDP Authority,[64] but is an entirely different document from a Data Breach Notification that must also be delivered to the PDP Authority. While the documentation process provides some leeway in the Data Breach Notification timeline and room for Data Controller to identify risk, we criticise the current draft wording as it provides an unclear scope on the documentation process, essentially enabling an indefinite period before the obligation to conduct notification arises. If the 3 x 24 hours deadline starts only after a formal conclusion was made by the Data Controller, there is a possibility for the Data Controller to delay as much as they can before finalising the documentation process. Below is the example to illustrate the Data Breach Notification timeline:

> On 8 January 2024, a Digital Bank experienced a Ransomware attack which locked users and operators from the system – essentially creating system failure. Pursuant to Permenkominfo/PSE regime, the latest date a Data Breach Notification had to be provided was 14 days after the date which was 22 January 2024. However, under UU PDP and current RPP PDP, the 3 x 24 deadline only started after the formal documentation process had been concluded by the Digital Bank. In practice, a formal documentation process could take months and even years to materialise. This is the case during a Bank of Ireland cyber incident, where a breach has been known by the Bank since 26 April 2019 while a final internal investigation was concluded on 6 March 2020, almost a year after the breach was discovered.[65] As a

[63] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 125 Paragraph (1) and (2).

[64] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 125 Paragraph (2).

[65] Irish Personal Data Protection Commission, Decision on IN-19-9-5, 59.

result, there needs to be further supervision on the documentation stage before leading to notification as this paper will recommend Section IV for Indonesia's Data Protection Authority in ensuring a reasonable timeline of Data Breach Notification.

Additionally, the legal relationship between Data Processor and Data Controller adds to the complexity of conducting Data Breach Notification, especially in the context of financial services arrangements. For instance, Banking institutions that directly collect Personal Data from their customers may require the involvement of other entities such as payment services infrastructure or third-party vendors that add more layers to incident response management.[66] Banking institutions acting as Data Controllers have the obligation to regularly supervise Personal Data processing by third parties that provide assistance to the institutions on their behalf.[67] However, an additional obligation arises in the case of a Data Breach on a Data Processor's side (for instance, a company providing cloud storage hosting suffers a data breach, and an Indonesian Bank utilises that company services to store consumer and employee data).[68] The duty to notify the supervisory authority and Data Subjects remains with the bank as its principal, however the cloud-services company has an obligation to notify any failure of Personal Data to the Data Controller in the first instance. As the term "first instance" is not clarified under RPP PDP, it is important to establish a clearly defined workflow and procedure of notification during cyber incidents under the mandatory Data Processing Agreement among all parties to establish rights and obligations thereunder. [69] Reflecting on EDPB Guideline 9/2023, the European Data Protection Board added an example where Data Processors can send out Data Breach Notifications on behalf of the controller as long as proper authorization from the Controller has been made within the contractual terms.[70]

Moving to the last regulation, the recently enacted Circular Letter 29/SEOJK.03/2022 on Cyber Security and Resilience outlines mandatory security testing and assessments for Banks, but also lays out detailed procedures of

[66] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 133 Paragraph (1) and (2).

[67] Indonesia, "*Personal Data Protection Law*," Article 37.

[68] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 162.

[69] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 21.

[70] "Guidelines 9/2022 on personal Data Breach Notification under GDPR," European Data Protection Board, accessed February 8th, 2024, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

Data Breach Notification to the Financial Services Authority as a relevant supervisory authority when data breach occurred in the financial sectors. Similar to Permenkominfo/PSE regime, the trigger arises when a cybersecurity incident arises, defined as "attempts, activity, and/or action that cause electronic system to function not as intended, for instance due to Malware, Web Defacement, and Distributed Denial of Services." [71] When such an incident occurs, banks are required to notify the Financial Services Authority in two stages.

First, is Initial Cyber Incident Notification that must be reported within 24 hours after the incident is known, the report contains all available information at early stage regarding cyber incident to the Bank,[72] (i) such as timing of the incident; (ii) when the incident is known; (iii) type of cyber incident (malware, hacking, Ransomware, defacement, etc); (iv) the name of system or server as incident entry point; (v) initial response after cyber incident; and (vi) initial impact assessment. This Initial Cyber Incident Notification can be delivered electronically to the Financial Services Authority, and the Bank must ensure the notification is received properly by the authority.[73] Subsequently, Bank have the obligation to deliver Cyber Incident Report which must include 29 questions in total related to information on the data breach point of contact/reporter, general information of the cyber incident; assessment on the cyber incident to bank; chronological information of the incident, analysis on the cause of incident; final analysis which includes restorative plans and the target date to solve the issue.[74] This final report must be delivered through the Financial Services Authority reporting system at maximum five working days after the cyber incident is discovered.[75]

Requirements under Circular Letter 29/SEOJK.03/2022 stands independent of any other data breach notification requirements that are in place, such as what is stipulated under Permenkominfo 20/2016 and PDP Law 27/2022. As OJK requirements are more comprehensive compared to the other laws, these can be seen as best practices adopted into the banking industry and financial services institutions. However, it raises the issue of regulatory overlap when Permenkominfo 20/2016, UU PDP, and sectoral regulations significantly diverge either in the content of notification in addition to the timeline.[76] This will be dissected further under Section IV.

---

[71] Financial Services Authority, Circular Letter 29/SEOJK.03/2022 on Cyber Security and Resilience, 16-17.

[72] Financial, Circular Letter 29/SEOJK.03/2022, 17.

[73] Financial, Circular Letter 29/SEOJK.03/2022, 17.

[74] Financial, Circular Letter 29/SEOJK.03/2022, 85-87.

[75] Financial, Circular Letter 29/SEOJK.03/2022, 85.

[76] Pursuant to Circular Letter 29/SEOJK.03/2022 on Cyber Security and Resilience, if other authority regulates the timeline of Initial Cyber Incident Notification or Cyber Incident Report with a longer timeline, the timeline within Circular Letter must be adhered to.

II.A.1. The EU GDPR Perspective and Practices on Data Breach Notification

As a comparison with which to understand the depth of Data Breach Notification requirements, the EU GDPR as a more mature privacy jurisdiction has established various jurisprudence and guidelines to supplement the interpretation of procedures. After the EU GDPR came into effect in 2018, there have been more than 160.000 Data Breach notifications in the jurisdiction with a daily average of 335 breach notifications received by Data Protection Authorities in the region.[77] While EU GDPR is not directly applicable in Indonesia, UU PDP itself is drafted with EU GDPR framework due to the more developed practices of the jurisdiction.[78] Thus, there are lessons learned in the normative framework and established practice under EU GDPR.

Under the GDPR, Data Breach Notifications to the Supervisory Authority are governed under Article 33 of the EU GDPR, while delivery to Data Subjects are governed under Article 34 GDPR. In addition to the separate article regarding Data breach Notification, the European Data Protection Board has also published Guideline 9/2022 on Personal Data Breach Notifications in order to clarify persisting issues in practice.[79]

As a start, not all data breaches[80] trigger Data Breach Notification to Supervisory Authority or Data Subjects. Pursuant to Article 33 EU GDPR, only data breaches that present a risk to the rights and freedoms of natural persons must be notified to the Supervisory Authority without undue delay or no more than 72 hours.[81] In turn, Article 34 EU GDPR provided that requirement to notify Data Subjects only arises when the data breach presents a **high-risk to the rights and freedoms of natural persons**. This is also supplemented by Article 34 (2) EU GDPR, which establishes scenarios where a data breach does not need to trigger notification requirements, where:[82]

---

[77] DLA Piper Report, "DLA Piper GDPR Fines and Data Breach Survey: January 2024," accessed 8 February 2024, https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024.

[78] Pratiwi Agustini, "PDP Law will facilitate data exchange with other countries," Directorate General of Informatics Applications, accessed 8 February 2024, https://aptika.kominfo.go.id/2020/11/uu-pdp-akan-permudah-pertukaran-data-dengan-negara-lain/.

[79] Lou Mailhac, "The EDPB updates the WP29 guidance on personal data breach notification," Lexology, accessed 8 February 2024, https://www.lexology.com/library/detail.aspx?g=c95a7003-2cd1-4694-a78c-12374adc7254.

[80] Pursuant to GDPR, Article 4 Paragraph 12 defined as breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

[81] European Union, "General Data Protection Regulation," Regulation 2016/679, Article 33.

[82] European Union, "General Data Protection Regulation," Regulation 2016/679, Article 34 Paragraph (2).

1. There has been appropriate technical and organisational protection measures applicable to the Personal Data affected by the breach, for instance rendering personal data unintelligible to any person who is not authorised to access it, such as encryption;
2. The controller has taken subsequent measures to the point that high-risk to the rights and freedoms of Data Subject no longer likely to materialise; and
3. Disproportionate effort would be required, a public communication or similar would suffice to inform Data Subjects in an equally effective manner.

Following this, the next burning question under EU GDPR is how to determine the risk posed to individuals when a Data Breach has occurred. EDPB Guideline 9/2022 provides that the logic or assessment to determine whether or not a data breach would pose a risk, high risk, or be exempted is to be conducted by the organisation experiencing data breach itself, with a comment that there needs to be an internal documentation process in the case that the data breach will not be notified.[83] This also aligns with Article 34 Paragraph (4) EU GDPR as a control mechanism, where Supervisory Authority can instruct the Data Controller to conduct Data Breach Notification to the Data Subject based on the provided documentation, even if the initial conclusion is not high risk.[84]

Documentation is essential for companies, not only as a way to ensure preventive measures can be taken for similar incidents but also as fulfilment of accountability principles to the Data Protection Authority. The incident documentation is often requested in hearings by the Data Protection Authority in the European Union, pursuant to EU GDPR Article 33 Paragraph (5) "the controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and remedial action taken. That documentation enables the supervisory authority to verify compliance within this Article."[85] The DPA considered that the accountability principle is applicable in cyber incidents through conducting proper documentation processes that can demonstrate that all necessary actions have been taken to set out technical and organisational measures throughout the incident, thus failure to conduct proper documentation would result in failure of Articles 33 and 34 of GDPR.[86]

---

[83] "Guidelines 9/2022 on personal Data Breach Notification under GDPR," Paragraph 125-126, European Data Protection Board, accessed 8 February 2024, https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

[84] European Union, "General Data Protection Regulation," Regulation 2016/679, Article 34 Paragraph (4).

[85] European Union, "General Data Protection Regulation," Regulation 2016/679, Article 33 Paragraph (5).

[86] "APD/GBA (Belgium) – 05/2021," Paragraph 46, GDPRhub, accessed February 8th, 2024, https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_05/2021.

Initially, the decision to trigger a notification should be mainly decided by the Data Controller as the party who is in the best position to assess the risk while the Data Protection Authority can provide recommendations on the risk assessments.[87] However, almost six years after GDPR came into force, the threshold to determine "risk" remains open to interpretation, leading to many organisations underreporting the breach due to increasing possibility of legal action and the rise of administrative fines.[88]

There is no clear methodology to assess risk posed to the rights and freedoms of natural persons under EU GDPR. Prior commentaries on Article 33 and Article 34 EU GDPR have heavily criticised the regulation for failing to distinguish "risk" and "high risk" situations, especially in the context of determining the threshold for mandatory Data Breach Notification.[89] Burdon, Reid, and Low argued that the initial distinction between "risk" and "high risk" is to prevent a notification fatigue where Data Subjects will experience a diluted perspective if all technical or organisational failures are being notified.[90] In a similar vein, conducting too many Data Breach Notifications with irrelevant risks will deplete significant resources from Data Protection Authorities which need to respond and act accordingly to the delivered notifications. As a middle ground, EDPB Guideline 9/2022 recommends utilising the following criteria for Data Controller in assessing the level of risk during data breaches:[91]

1. The type of breach;
2. The nature, sensitivity, and volume of Personal Data;
3. The ease of identification of individuals;
4. The severity of consequences to individuals; and
5. Special characteristics of affected individuals.

In 2022, the Belgian Data Protection Authority (*Gegevensbeschermingsautoriteit*) began utilising the proposed risk framework under the guideline to determine whether a breach would result in a high-risk against the rights and freedoms of a natural persons, even if the breach relates only to a single individual. Alternatively, Data Controllers can also utilise the European Union Agency for Network and Information Security that has proposed a methodology for assessing severity of Personal Data breach since 2013.[92]

---

[87] "Data breach notifications in the EU," European Network and Information Security Agency, 18, accessed 8 February 2024, https://www.enisa.europa.eu/publications/dbn/@@download/fullReport.

[88] DLA, "DLA Piper GDPR," 6.

[89] https://www.duo.uio.no/bitstream/handle/10852/84194/1/ICTLTHESIS---Candidate-8012.pdf, 27.

[90] Bernold Nieuwesteeg and Michael Faure, "An Analysis of the Effectiveness of the EU Data Breach Notification Obligation," *Computer & Law Security Review* 34 (2018): 1237.

[91] "Guidelines 9/2022," Paragraph 103-119.

[92] "APD/GBA (Belgium) – 05/2021," Paragraph 41.

Should a Data Breach Notification be considered mandatory, the next stage is ensuring the following elements must be present within the notification: i) nature of personal Data Breach, and additional information if possible such as the number of data subject concern, categories, and number of records affected; ii) name, and contact details of Data Protection Officers or other contact point; iii) description on the likely consequences of the data breach; and iv) description on the measures taken or proposed to be taken in addressing the breach, including mitigation measures.[93] There is no obligation for this notification to be fully accurate as it should only reflect the real-time information, considering the strict nature of Data Breach Notification under EU GDPR. To accommodate this, an emerging practice of dual-stage notification has been commonly accepted. In the first 72 hours of cyber incidents, organisations are required to focus on containing the breach and ensuring no mitigation steps are properly taken, organisations can conduct Data Breach Notification with the minimum requirements mandated by the law during the 72 hours period while conveying a more complete report beyond the timeline.[94] This is similar to the existing initial and final notification found under Circular Letter 29/SEOJK.03/2022.

To shed light on the triggers of Data Breach Notification and the notification procedures in practice, Table 2 below summarises decisions made by Data Protection Authorities within the European Union.

There are three key takeaways from the above decisions made by various EU Data Protection Authorities. First, the Data Controller does not need to wait until all affected data subjects are identified before sending Data Breach Notifications. Second, Data Controllers need to utilize public announcement through the website carefully as it does not necessarily erase its initial obligation to notify Data Subjects individually. Third, there is no minimum requirement for the duration or scale of an actionable Data Breach, every single breach that poses high-risk even to an individual would need to have Data Breach Notification sent out. While the practices are non-binding, this could shape as a practical guideline in Data Breach Notification in Indonesia both to the Supervisory Authority and to the Data Subjects.

[93] European Union, "General Data Protection Regulation," Regulation 2016/679, Article 33 Paragraph (3) and Article 34 Paragraph (2).

[94] Ralph O' Brien, "Privacy and Security: The New European Data Protection Regulation and It's Data Breach Notification Requirements," *Business Information Review*, 33, no. 2 (2016): 83.

Table 2.
EU GDPR Data Breach Notifications Decisions

No.	Data Protection Authority/Case Number	Case Summary	Results
1.	Datatilsynet (Denmark) - 2020-441-4364	A company notified data breach to Data Subject; however, the notification did not reach all related Data Subjects in addition to not including information such as the: (i) likely consequences of the breach; (ii) the indication of the period of the breach.	Datatilsynet (Denmark Data Protection Authority) concluded that the company has failed to meet the minimum requirements that must be included under Data Breach Notification. The minimum information is needed to enable Data Subjects in taking mitigative measures to prevent possible harm attributed to the breach. Datatilsynet did not impose administrative fines but ordered the company to take corrective measures.[95]
2.	Tietosuojavaltuutetun toimisto (Finland) - 2437/161/22	A public institution experienced a data breach due to Pegasus Spyware on 24 January 2022 but fails to inform it to the Data Protection Authority without undue delay or within the 72 hours' time limit after the breach has been known.[96] The public institution argued that it needs to finish an investigation and gain reasonable assurance, before conducting Data Breach Notification to the supervisory authority. Thus, the notification was	Tietosuojavaltuutetun toimisto (Finland Data Protection Authority) concludes that even if the Data Controller cannot provide all information of the breach within 72 hours, it still needs to conduct a notification in several stages to the supervisory authority.[97] Thus a violation of Articles 33 and 34 EU GDPR has occurred. Tietosuojavaltuutetun toimisto (Finland Data Protection Authority) did not impose an administrative fine.[98]

[95] "Case No. 2020-441-4364", Datalysisnet (Danish Data Protection Authority), accessed February 8th, 2024, https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/nov/sikkerhedsbrud-hos-zoo.

[96] Tietosuojavaltuutetun toimisto (Finland Data Protection Authority), Decision of the Deputy Data Protection Commissioner Case ID Number 2437/161/22, 1.

[97] Tietosuojavaltuutetun, Case ID Number 2437/161/22, 4.

[98] Tietosuojavaltuutetun, Case ID Number 2437/161/22, 7.

Table 2.
EU GDPR Data Breach Notifications Decisions Continued

No.	Data Protection Authority/Case Number	Case Summary	Results
3.	Gegevensbeschermingsautoriteit (Belgium) -DOS-2019-0486705/2021	In a technical error, a company accidentally switched a Data Subject's phone number to an unaffiliated third party for a period of four days. The accident gave the opportunity to the third party to access Data Subject's WhatsApp application and other various Personal Data associated with the phone number. The company argued there is no obligation to conduct Data Breach Notification to supervisory authority and data subject, as the breach only concerned a single individual for a short duration, with no sensitive data involved.[99]	APB/GBA (Belgium Data Protection Authority) concluded that even if a data breach relates only to a single person, it would have still fulfilled the threshold of mandatory Data Breach Notification as long as it could result in a serious consequence to the person[100] APB/GBA (Belgium Data Protection Authority) imposed an administrative fine of **25,000 on the** company.[101]
4.	DPC (Ireland) - DPC Case Reference: IN-19-9-5 BN-19-1-25	A banking institution accidentally uploaded erroneous customer data to the Central Credit Register, causing an unauthorized disclosure of Personal Data. The banking institution was aware of the breach on 22 January 2019 and notified the Irish Data Protection Commission with an indication of high-risk breach. However, the bank waited until technical action to remediate the breach on 5 December 2019, before deciding to conduct Data Breach Notifications to 236 Data Subjects.[102]	Irish Data Protection Commission concluded that communication Data Breach Notification, especially in the case related to financial data is necessary to enable Data Subject in mitigating the consequences of the breach. The delay of notification is almost 10 months since the breach has been known, resulting in the violation of Article 34 EU GDPR.[103] The Irish Data Protection Commission did not impose administrative fines due to the small number of data subjects affected and the less severe delay in communicating the breach when compared to other cases (BN-19-4-490).[104]

[99] Gegevensbeschermingsautoriteit, Case Number -DOS-2019-04867, Paragraph 40, 15.
[100] Gegevensbeschermingsautoriteit (Belgium Data Protection Authority), Case Number -DOS-2019-04867, Paragraph 41, 15.
[101] Gegevensbeschermingsautoriteit, Case Number -DOS-2019-04867, 22.
[102] Irish Personal Data Protection Commission, Decision on IN-19-9-5, 27-28.
[103] Irish, Decision on IN-19-9-5, 29.
[104] Irish, Decision on IN-19-9-5, 29.

Table 2.
EU GDPR Data Breach Notifications Decisions Continued

No.	Data Protection Authority/Case Number	Case Summary	Results
5.	DPC (Ireland) - DPC Case Reference: IN-19-9-5 BN-19-4-490	A banking institution incorrectly attributed over 47.000 Data subjects with a "Restructuring Event" status that leads to reduced creditworthiness. The banking institution was aware of the breach from 26 April 2019, but only started conducting Data Breach Notification to Data Subjects at the end of November 2020.[105]	The Irish Data Protection Commission concluded that the length it took to identify numbers of individuals affected; failure to communicate the Data Breach in a timely manner; and postponing communication until the establishment of the total number of individuals affected by the breach has violated Article 34 EU GDPR. Irish Data Protection determined that, even if further investigation needs to be concluded to accurately establish the number of affected individuals, the banking institutions should have notified Data Subjects earlier without waiting for a complete list of affected individuals.[106] Irish Data Protection Commission imposed an administrative fine of **€125.000.**
6.	Commissioner (Cyprus) - 11.17.001.010.007	A company has suffered data breach; however, the company only provides public announcement of the Data Breach Notification, without addressing individual Data Breach Notification. A Data Subject that received the news from a third party, complained that it has not received a Data Breach Notification where it should have been appropriate. The company argues that there is no indication to which individuals are affected by the breach. Thus, a public announcement would have been sufficient.[107]	Cyprus DPA concluded that the company should have conducted Data Breach Notification directly to the affected Data Subjects, by leveraging existing registered user emails in the company. This is strengthened by the fact that the company is processing sensitive data, such as the sex lives of its registered users.[108] Cyprus DPA found a violation of Article 34 GDPR, but only issued reprimands without administrative fines.[109]

[105] Irish, Decision on IN-19-9-5, 59.

[106] Irish, Decision on IN-19-9-5, 32.

[107] "Stripchat reprimanded for 64.694.953 account breach," Floort.net, accessed February 8th, 2024, https://floort.net/posts/stripchat_data_breach/.

[108] Office of the Commissioner for Personal Data Protection Republic of Cyprus, Decision Requesting Excessive Identification Information to Comply to a Subject Access Request by Technius Ltd, Case Ref 11.17.001.010.007, 6, https://drive.google.com/file/d/1nL7rkTZ8BT3srqKXYX2rk18Ib8I8xDXb/view?usp=sharing

[109] Cyprus, Decision Requesting, 6.

When compared to Indonesia, the only notable difference between UU PDP and EU GDPR is the trigger for requiring Data Breach Notification. As the metrics established under Article 124 RPP PDP is only to consider whether there has been Personal Data disclosure without mandatory risk matrix assessment under Article 33 and Article 34 EU GDPR.[110] This approach circumvents the "risk" and "high risk" debate entirely by focusing on the actual consequences of a cyber incident. While the regulation remains as a draft, this mechanism would prove ineffective in the context of Ransomware attacks where a breach or cyber incident has been clearly announced to the public while the data disclosure (*pengungkapa*n) follows only if the companies failed in negotiation. As the requirement of notification only manifests after the disclosure has occurred, Data Subjects will remain helpless after the Ransomware group announced their clear intention. Thus, in many future scenarios, Indonesia's Data Breach Notification will be "too late, too ineffective" if the Article 124 RPP PDP remained as is in the final implementing regulations of UU PDP.

All in all, the rules and guidelines gathered can provide guidance on drafting a proper data breach notification. An interesting note is that data breach notification should also be sent to the "supervisory authority". However, in Indonesia – who exactly is the leading supervisory authority regarding data protection and privacy violations?

IV. REGULATORY COMPLEXITIES IN DATA BREACH NOTIFICATION: ONE-STOP NOTIFICATION MODEL FOR INDONESIA'S PERSONAL DATA PROTECTION AUTHORITY

Indonesia's Personal Data Protection Authority will play a key role as an institution that oversees compliance with UU PDP and its implementing regulation. Under EU GDPR, Garante in Italy, Irish DPC in Ireland, and AP in the Netherlands are highly active in monitoring and providing sanctions for violations of the EU GDPR.[111] In the context of data breaches, these supervisory authorities are well-equipped with the know-how on managing notifications that have been informed from Data Controllers.[112] In an Indonesian twist, almost two years since UU PDP was legislated, the fate of Indonesia's Personal Data Protection Authority remains unclear as only the

[110] Indonesia, *Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law,"* Article 124.

[111] Brian Daigle and Mahnaz Khan, "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities," *Journal of International Commerce & Economics* 2020: 9-13.

[112] "Breach Notification," Data Protection Commission, accessed 8 February 2024, https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification.

necessary Presidential Regulation to establish this institution have yet to be enacted. As a consequence, a single Data Breach in 2023 would trigger an ad-hoc engagement from Data Controller to every single other institution that might be relevant, with every institution requiring different notification procedure and format:

Table 3.
Data Breach Notification Procedures and Timeline to Supervisory Authority in Indonesia Continued

No.	Authority	Procedure and Notification Timeline	Remarks
1.	Personal Data Protection Authority	Procedure is not available as of writing. Notification must be informed to Personal Data Protection Authority **within 3x24 hours after a cyber incident is known.**	RPP PDP did not mention whether the procedure will be stipulated further under PDP Authority regulation
2.	Badan Siber dan Sandi Negara	Applicable to all cyber incident 1) Report is submitted through hotline calls at 02178833610 or email to bantuan70@bssn.go.id. 2) Report must include the identity of reporter supported by the evidence of cyber incident (photo/screenshot/log file) 3) BSSN will provide confirmation of report submission 4) BSSN will conduct observation and investigation over the report 5) BSSN will provide recommendation in handling the cyber incident 6) BSSN can be involved to act upon the cyber incident if the IT administrator/asset owner cannot solve the cyber incident independently.	Guideline is available at https://www.bssn.go.id/aduan-siber/

Table 3.
Data Breach Notification Procedures and Timeline to Supervisory Authority in Indonesia Continued

No.	Authority	Procedure and Notification Timeline	Remarks
		Applicable to cyber incident on Vital Information Infrastructure 1) Organization's Cyber Incident Response Team must report to Sector Cyber Incident Report Team within 1x24 hours after the incident is known. 2) The Report must be forwarded to National Cyber Incident Team under BSSN within the same timeline.	Presidential Regulation No. 82 Year 2022 on Vital Information Infrastructure As of writing, there is no public list of Electronic System classified as Vital Information Infrastructure to determine whether this procedure applies to an organisation or not. Within the Financial Sector, the Sectoral Incident Report Team is OJK-CSIRT
3.	Ministry of Communication and Information	Ministry of Communication and Information will provide a link to "Alleged Data Breach Report Form." However, this electronic submission form is not accessible publicly. In practice, companies experiencing data breach must manually liaise with the Ministry of Communication and Information through email. Electronic System Provider must conduct **Data Breach Notification within 14 (fourteen) days after breach is known.**	It usually took more than 3 x 24 hours to liaise with the Ministry of Communication and Information. It remains unclear whether liaising to Ministry of Communication and Information will utilise the 14 (fourteen) days after breach is known under PP PSE/ Permenkominfo or 3 (three) days after the breach is known under UU PDP
4.	Financial Services Authority	**Initial Cyber Incident Notification must be reported within 24 hours** after the breach is known electronically to the Financial Services Authority. **Cyber Incident Report must be reported within 5 working days** after the breach is known to the Financial Services Authority reporting system.	No publicly available information is found on the recipient or address to OJK reporting system to deliver both Initial Cyber Incident Notification and Cyber Incident Report.

Table 3.
Data Breach Notification Procedures and Timeline to Supervisory Authority in Indonesia Continued

No.	Authority	Procedure and Notification Timeline	Remarks
5.	Indonesian National Police	No specific procedures, but all cybercrimes are advised to be reported to the Directorate of Cyber Crime. This will be followed by an investigation by the Directorate's Computer Security Incident Response Team.[113]	Submission form is available at https:/patrolisiber.id/

As established under Section III, what constitutes "Failure" under UU ITE/Permenkominfo regime differs from UU PDP in addition to the sectoral regulations under Indonesian Financial Services Authority, this is also the case of diverging timeline to trigger Data Breach Notification between the regulations. A banking and financial services institution has no guidance on whether it should only notify the Financial Services Authority as its direct supervisor or also need to go through the cumbersome procedure of notifying every single authority to ensure bulletproof compliance. Notification process would have cost significant resources, while failing to notify might result in administrative sanction from the supervisory authorities.[114]As a solution, a harmonising effort is necessary to deal with the gap between regulations.

The last minute scramble which results in a jarring procedural hassle every time a breach occurs can be avoided, if Indonesia commits itself into having a leading Personal Data Protection Authority as mandated under Article 58 UU PDP.[115] A single institution that is envisioned to wield the power in formulating strategies and policies related to Personal Data Protection that will become the central lead in guiding compliance up to imposing administrative sanctions where possible.[116] Specifically, Article 60 UU PDP authorised Indonesia's Personal Data Protection Authority to as the following:[117]

[113] "Police Investigate Alleged Hacking of 204 million Permanent Voter List Data at the General Election Commission," Metrotvnews.com, accessed February 9th, 2024, https://www.metrotvnews.com/play/bJECaroO-polri-usut-dugaan-peretasan-204-juta-data-dpt-di-kpu.

[114] Indonesia, "*Personal Data Protection Law*," Article 57.

[115] Article 58 UU PDP.

[116] Article 59 UU PDP.

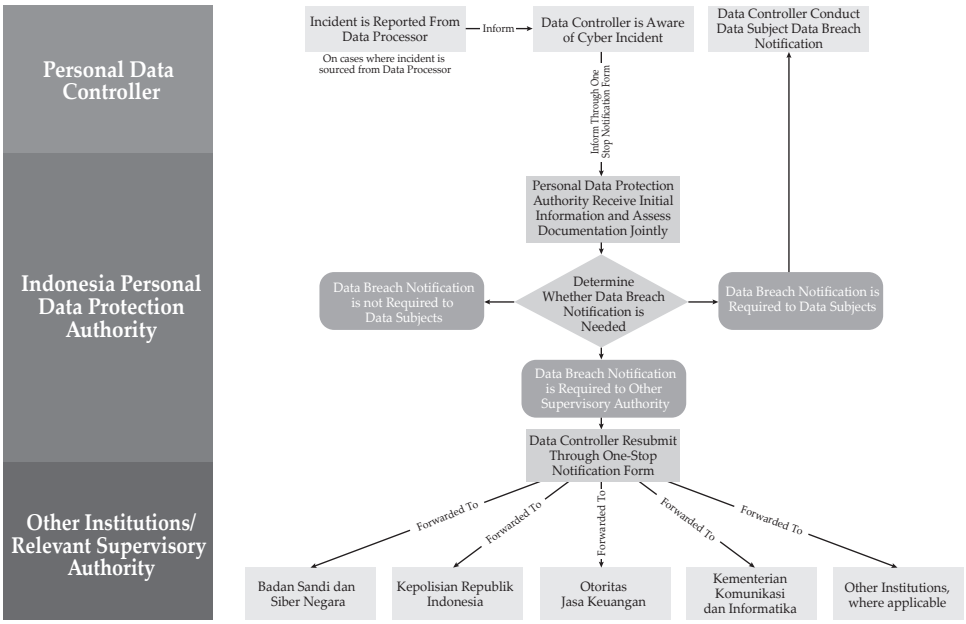
[117] Article 60 UU PDP.

a. Formulate and stipulate policies in the area of Personal Data Protection;
b. Supervise the compliance of Personal Data Protection;
c. Impose administrative sanction on Personal Data Protection violations;
d. Assist the law enforcement in handling allegation of Personal Data crimes;
e. Cooperates with other Personal Data Authority to facilitate cross-border issues;
f. Assess whether the requirement for cross-border data transfer has been satisfied;
g. Enact order as a follow-up of supervision by Data Controller and Data Processor;
h. Establish publication of supervision results;
i. Receive complaints and/or report alleged to Personal Data Protection violations;
j. Conduct inspection and searchers upon complaints, reports, and/or supervision results of alleged Personal Data Protection violations;
k. Summon any person and/or public agency related to possible Personal Data Protection violation;
l. Request statement, data, information, and document from any person and/or public institution related to possible Personal Data Protection violations;
m. Summon any experts that are necessary in the inspection and search related to alleged Personal Data Protection violation;
n. Conduct an inspection and search against electronic systems, facilities, room, and/or places used by Data Controller and Data Processor, this includes obtaining access to data and appointing third party; and
o. Request legal assistance from the Attorney General in Personal Data Protection dispute.

As of February 2024, the fragmented procedure to conduct Data Breach Notification to various supervisory authorities has not only created uncertainty among Data Controllers to determine which authority needs to be notified, the diverging formats of notification to each institution, and costs a significant amount of time in manually liaising to each authority. Organizations experiencing data breach already have to juggle with limited resources to contain the incident, assess the impact of the breach, and conduct recovery or documentation of the attack.[118] Therefore, the existing patchwork procedure of Data Breach Notification will cost significant resources by the Data Controller. In response to this, we propose that Indonesia's Personal Data Protection Authority to utilize One-Stop-Notification Model:

[118] Nivedita Shinde and Priti Kulkarni, "Cyber Incident Response and Planning: A Flexible Approach," *Computer Fraud & Security* no. 1 (2021): 16.

Figure 1. One-Stop Notification Model for Data Breach Notification



Under the One-Stop-Notification Model, the Data Controller must inform the Personal Data Protection Authority as soon as possible after knowing the existence of the breach. This process will be considered a part of initial documentation procedure maintained under Article 125 RPP,[119] and separate from the official Data Breach Notification to Supervisory Authority maintained under Article 46 UU PDP.[120]

The involvement of the Personal Data Protection Authority at the early stage of the incident would provide three concrete benefits. *First*, it would provide better room for assessing the actual impact of the breach, for instance Data Controller may initially determine that the breach does not result in the compromise of Personal Data,[121] while the Personal Data Protection Authority may determine otherwise. This will eventually reduce the high possibility of the Data Controller underreporting the impact of the breach. *Second*, liaising with Personal Data Protection Authority would take into account our initial concern under Section III.B where Data Controller may abuse the unspecified deadline of conducting documentation process which could result in an indefinite amount of period before obligation to conduct notification arises, if Article 125 RPP PDP timeline remains open to interpretation – the

[119] Indonesia, "*Draft Regulation on Government Regulation on the Implementation of Personal Data Protection Law* , Article 125.

[120] Indonesia, "*Personal Data Protection Law*," Article 46.

[121] DLA, "DLA Piper GDPR Fines and Data Breach," 6.

Personal Data Protection Authority can provide recommendations to the Data Controller regarding the time needed to conclude documentation process on a case-by-case basis. In the context of Ransomware attacks, Data Controllers who are being extorted by malicious actors can communicate effectively with the Personal Data Protection Authority, the latter could provide advice or recommendation in dealing with the Ransomware groups to prevent ransom payment. Thus, breaking the vicious cycle of Ransomware extortion tactics.

Lastly, the existing issue of patchwork notification procedures to other supervisory authorities can be circumvented if the One-Stop-Notification-Model could connect the notification submitted to the Personal Data Protection Authority to the relevant supervisory authority. For instance, a Major Bank needs to inform the Personal Data Protection Authority, Ministry of Communication and Information, and the Financial Services Authority but does not have access to any link or network to the notification procedures of the other institution as highlighted in Table 3. After submitting through One-Stop-Notification form, Indonesia Personal Data Protection Authority can determine if another supervisory authority needs to be notified and connect the submission form of another supervisory authority within the One-Stop-Notification Form. The challenge to this proposal is the existing patchwork notification procedure that needs to be harmonised, therefore additional amendments to existing sectoral regulations is required to enable the involvement of Indonesia's Personal Data Protection Authority in centralising the data breach notification procedure.

The proposed One-Stop-Notification Model build from smart thresholds approach proposed by Nieuwesteeg and Faure which put a stronger emphasis on Data Protection Authority role to become the major player in assisting data controllers to determine whether Data Subjects need to be notified, owing to the fact that DPA will have more expertise in determining whether an action is needed, understood the impact of the breach, and are able to prevent data subject's notification fatigue as the DPA would know how any notifications have been send previously to data subjects.[122] Further, the model is partially inspired by Dutch-DPA electronic Data Breach Notification form that assists Data Controller in submitting initial notification, while also requiring the declaration of whether other supervisory authority has been notified.[123] We take the Dutch-DPA model one step further by connecting Data Breach Notification to supervisory authority to ensure no notification is missing.

[122] Bernold, "An Analysis," 1244-1245.

[123] "Meldformulier datalekken," Autoriteit Persoonsgegevens, accessed 8 February 2024, https://datalekken.autoriteitpersoonsgegevens.nl/.

V. CONCLUDING REMARKS

Banks and other financial services providers are businesses rely on the trust of their customers. As a highly regulated sector, a practice of good corporate governance is imperative in banking to reduce the credit risk, market risk, operational risk, and reputational risk. However, when a new technology is introduced, be it in the form of digital banking, payment system, or even operational platforms, will introduce cyber risk which affects all the previously mentioned risk. Malicious cyber actors such as Ransomware organisations pose a threat to the new opportunities, highlighted as one of the most lucrative cyberattacks throughout the years. Banking and financial institutions remain the most targeted organisations due to the sheer amount of sensitive financial data and strategic assets it processed, Ransomware attacks also have the capability to shut down strategic infrastructure, thus forcing organisations to either pay ransom or risk further exploits.

UU ITE, alongside relevant regulations such as PP 81/2019 and Permenkominfo 20/2016 have acted as the initial framework for organisations compliance with cybersecurity and privacy regulations. Further, the enactment of UU PDP has explored more details on the framework of personal data protection which also enhances additional cybersecurity and data protection requirements that companies must adhere to, such as enabling access management or appropriate encryption throughout Personal Data collection, use, storage, transfer, and erasure. These new requirements, which are also further detailed on the latest version of RPP PDP, can serve as a starting point to ensure a proper cybersecurity and personal data protection framework of organisations. Banking and other financial services providers must also take into account waves of new regulations both from Bank Indonesia and Financial Services Authority that often mandates a stricter requirement, reflecting the importance of safeguarding trust and consumer data in the area.

This paper has analysed the complexities between the new regulations, which will result in procedural challenges regarding Data Breach Notification. Every single regulation provides a different trigger, timeline, and procedure in order to conduct an appropriate notification to Data Subjects and Supervisory Authority. The existing practice also provides no clear framework, as it stands now, a data breach notification process is cumbersome as an organisation must manually contact the relevant Supervisory independently and separately.

In the spirit of welcoming Indonesia's Personal Data Protection Authority, this paper proposes a model that sets a central role of this authority in managing Data Breach Notifications through One-Stop-Form mechanism. In our model, the Data Controller would cooperate closely with the authority in determining whether a data breach is notifiable and to whom notification should also be forwarded to. This model establishes a strong connection with

Personal Data Protection Authorities while also preventing Data Controllers from potentially abusing flexible timelines under UU PDP implementing regulation. Ergo, coordination on cyber incidents, can then be conducted with other relevant authorities such as Financial Services Authority and Indonesia Cyber and Crypto Agency to ensure necessary cooperation is reached to mitigate the damage and protects data subject from receiving any further harm such as phishing, data interception, and other cybersecurity threats through exploitation of leaked data.

REFERENCES

Bank Indonesia, "*Amendment of Regulation of the Members of the Board of Governors*," Regulation Number 20 of 2023 concerning the Implementation Procedure of Consumer Protection of Bank Indonesia, Article 3 Paragraph 1 Point f.

European Union. "General Data Protection Regulation." Regulation 2016/679.

Financial Services Authority, Circular Letter 29/SEOJK.03/2022 on Cyber Security and Resilience,

Gegevensbeschermingsautoriteit, Case Number -DOS-2019-04867, Paragraph 40, 15.

Indonesia. Electronic Information and Transactions Law. Law No. 11 of 2008. LN.2016/No.251, TLN No. 5952.

Indonesia. Electronic System and Transaction Operation Regulation. Government Regulation No. 71 of 2019.

Indonesia. Personal Data Protection Law. Law No. 27 of 2022. LN.2022/No.196, TLN No.6820.

Indonesia. Personal Data Protection Legislation Bill. Number 27 of 2022.

Indonesia. Presidential Regulation on Protection of Vital Information Infrastructure. Regulation No. 82 of 2022. LN.2022/No.129.

Indonesia. Protection of Personal Data in Electronic Systems Law. Regulation of the Minister of Communication and Information Technology No. 20 of 2016.

Irish Personal Data Protection Commission. Decision on IN-19-9-5.

"PRESS RELEASE BSI Branch, ATM & Mobile Banking Services Have Returned to Normal." Bank Syariah Indonesia. Accessed February 8, 2024. https://ir.bankbsi.co.id/newsroom/1a92cc8ca2_4364ce956d.pdf.

"PRESS RELEASE BSI President Director: We Apologize and Are Trying to Restore Services," Bank Syariah Indonesia, accessed February 8, 2024, https://ir.bankbsi.co.id/newsroom/dc70693fac_d7743dac9a.pdf.

"Press Release No. 256/HM/KOMINFO/08/2023 Drafting Implementing Rules, Kominfo Opens Public Participation Through the pdp.id." Public Relations Bureau of the Ministry of Communication and Information. Accessed February 8th, 2024. https://www.kominfo.go.id/content/detail/51157/siaran-pers-no-256hmkominfo082023-tentang-susun-aturan-pelaksana-kominfo-buka-partisipasi-publik-lewat-laman-pdpid/0/siaran_pers.

Tietosuojavaltuutetun toimisto (Finland Data Protection Authority). Decision of the Deputy Data Protection Commissioner. Case ID Number 2437/161/22, 1.

"83% of organizations paid up in ransomware attacks." VentureBeat. Accessed February 8th, 2024. https://venturebeat.com/security/83-of-organizations-paid-up-in-ransomware-attacks/.

"Advocate General Opinion in Case C-340/21, Press Release No. 67/23." Court of Justice of the European Union. Accessed 8th February 2024. https://curia.europa.eu/jcms/upload/docs/application/pdf/2023-04/cp230067en.pdf.

"APD/GBA (Belgium) – 05/2021," Paragraph 46. GDPRhub. Accessed February 8, 2024. https://gdprhub.eu/index.php?title=APD/GBA_(Belgium)_-_05/2021.

"Breach Notification." Data Protection Commission. Accessed February 8, 2024. https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification.

"Case No. 2020-441-4364." Datalysisnet (Danish Data Protection Authority). Accessed February 8, 2024. https://www.datatilsynet.dk/afgoerelser/afgoerelser/2020/nov/sikkerhedsbrud-hos-zoo.

"Dark Web Profile: LockBit 3.0 Ransomware." SOCRadar. Accessed February 8th, 2024. https://socradar.io/dark-web-profile-lockbit-3-0-ransomware/#:~:text=LockBit%203.0%20is%20a%20Ransomware,businesses%20and%20critical%20infrastructure%20organizations.

"Expert Calls Conti Ransomware Gang that Breached BI Dangerous Hackers." CNN Indonesia. Accessed February 8th, 2024. https://www.cnnindonesia.com/teknologi/20220120191930-185-749298/ahli-sebut-geng-ransomware-conti-yang-bobol-bi-peretas-berbahaya.

"Guidelines 9/2022 on personal Data Breach Notification under GDPR." European Data Protection Board. Accessed February 8th, 2024. https://edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf.

"LockBit hackers pocket 15 million BSI customer records, threaten to sell them if negotiations fail." Merdeka.com. Accessed 8 February 2024. https://www.merdeka.com/teknologi/hacker-lockbit-kantongi-15-juta-data-nasabah-bsi-ancam-dijual-jika-negosiasi-gagal.html.

"Meldformulier datalekken." Autoriteit Persoonsgegevens. Accessed February 8, 2024, https://datalekken.autoriteitpersoonsgegevens.nl/.

"NCCA Hearing Meeting with Commission I The House of Representatives of the Republic of Indonesia." National Cyber and Crypto Agency. Accessed February 8th, 2024. https://www.bssn.go.id/rapat-dengar-pendapat-bssn-bersama-komisi-i-dpr/.

"Police Investigate Alleged Hacking of 204 Million Permanent Voter List Data at the General Election Commission." Metrotvnews.com. Accessed February 9, 2024. https://www.metrotvnews.com/play/bJECaroO-polri-usut-dugaan-peretasan-204-juta-data-dpt-di-kpu.

"Stripchat reprimanded for 64.694.953 account breach." Floort.net. Accessed February 8, 2024. https://floort.net/posts/stripchat_data_breach/.

"The Prolificacy of LockBit Ransomware." The Hacker News. Accessed February 8, 2024. https://thehackernews.com/2023/03/the-prolificacy-of-lockbit-ransomware.html.

Agustini, Pratiwi. "PDP Law will facilitate data exchange with other countries." Directorate General of Informatics Applications. Accessed 8 February 2024,

Benmalek, Mourad. "Ransomware on cyber-physical systems: Taxonomies, case studies, security gaps, and open challenges." *Journal Internet of Things and Cyber-Physical Systems* 4 (January 2024): 186.

Brien, R. O. "Privacy and security: The new European data protection regulation and it's data breach notification requirements." *Business Information Review,* 30 (2016): 81-83.

Burton, Cedric. "Article 32: Security of Processing" in Christopher Kuner the EU General Data Protection Regulation: A Commentary (Oxford: Oxford University Press, 2020): 635-636.

Daigle, Brian and Mahnaz Khan. "The EU General Data Protection Regulation: An Analysis of Enforcement Trends by EU Data Protection Authorities." *Journal of International Commerce & Economics* 2020: 9-13.

Darem, Abdulbasit, et al., "Cyber threats classifications and countermeasures in banking and financial sector." *IEEE Access*, Vol. 11 (2023): 125139.

Delpiero, Maichle, et al., "Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban *Online Marketplace* dalam Pelindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data." *Padjadjaran Law Review*, 9, no. 1 (2021): 13-16.

DLA Piper Report. "DLA Piper GDPR Fines and Data Breach Survey: January 2024." Accessed 8 February 2024. https://www.dlapiper.com/en/insights/publications/2024/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2024.

Gotay, Anne. "How Ransomware Shakes Up GDPR Compliance." Sotero. Accessed 8 February 2024. https://www.soterosoft.com/blog/how-ransomware-shakes-up-gdpr-compliance/.

Greenleaf, Graham. "Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance." *169 Privacy Laws and Business International Report*, 1, 3-5 (2021).

Hallinan, Dara and Frederik Zuiderveen Borgesius. "Opinions Can Be Incorrect (in our opinion!) On Data Protection Law's Accuracy Principle." *International Data Privacy Law*, 10, no. 1 (2020): 2.

Kosta, Eleni. "Thematic Document: Security of Processing and Data Breach Notification." *European Data Protection Board* (November 2023): 8.

Lie, Gunardi, Dylan Aldianza Ramadhan, and Ahmad Redi. "Independent Commission of Personal Data Protection: Quasi-Judicial and Efforts to Create Right to be Forgotten in Indonesia." *Jurnal Yudisial*, 15, no. 2 (2022): 241-243.

Madnick, Mailhac, Lou. "The EDPB updates the WP29 guidance on personal data breach notification." Lexology. Accessed 8 February 2024. https://www.lexology.com/library/detail.aspx?g=c95a7003-2cd1-4694-a78c-12374adc7254.

Makarim, Edmon., "The Law Against Personal Data Leaks." *Public Relation of Faculty of Law Universitas Indonesia.* July 10, 2020. https://law.ui.ac.id/pertanggungjawaban-hukum-terhadap-kebocoran-data-pribadi-oleh-edmon-makarim/.

McGee, Marianne Kolbasuk, "Irish Authorities Levy GDPR Fine in Centric Health Breach." Bank Info Security. Accessed 8 February 2024. https://www.bankinfosecurity.com/irish-authorities-levy-gdpr-fine-in-centric-health-breach-a-21346.

Meurs, Tom, et al., "Deception in Double Extortion Ransomware Attacks: An Analysis on Profitability and Credibility." *Computers & Security* 138 (2024): 3.

Multazam, Mochammad Tanzil and Noor Fatimah Mediawati. "Personal Data Collection: Recent Developments in Indonesia." *2nd Virtual Conference on Social Science in Law, Political Issue and Economic Development* (2022): 52.

Nadir, Ibrahim and Taimur Bakshi. "Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques." *International Conference on Computing, Mathematics and Engineering Technologies* (2018): 5.

Nieuwesteeg, Bernold and Michael Faure. "An Analysis of the Effectiveness of the EU Data Breach Notification Obligation." *Computer & Law Security Review* No. 34 (2018): 1237.

Office of the Commissioner for Personal Data Protection Republic of Cyprus. Decision Requesting Excessive Identification Information to Comply to a Subject Access Request by Technius Ltd. Case Ref 11.17.001.010.007. https://drive.google.com/file/d/1nL7rkTZ8BT3srqKXYX2rk18Ib8I8xDXb/view?usp=sharing

Pratama, Erwin. "Negotiation period ends, LockBit reveals BSI data on the Dark Web." Tempo.co. Accessed 8 February 2024. https://tekno.tempo.co/read/1726219/masa-negosiasi-berakhir-lockbit-ungkap-data-bsi-di-dark-web.

Respati, Agustinus Rangga, Aprillia Ika. "NCCA Mentions the Potential for Cyber Attacks is Still High, Especially the "Ransomware Type." Kompas.com. Accessed February 8, 2024. https://money.kompas.com/read/2023/11/15/114406526/bssn-sebut-potensi-serangan-siber-masih-tinggi-terutama-jenis-ransomware.

Rosadi, Sinta Dewi. *Pembahasan UU Pelindungan Data Pribadi.* (Jakarta: Sinar Grafika, Rusmalina, Yunia. "Not Ransomware, BFI Finance Admits to Malware Attack." Bloomberg Technoz. Accessed 8 February 2024, https://www.bloombergtechnoz.com/detail-news/7300/bukan-ransomware-bfi-finance-akui-terkena-serangan-malware.

Ryan, Pierce, et. al., "Dynamics of Targeted Ransomware Negotiation." *IEEE Access*, 10 (2022): 32839.

Stuart E. "The Continued Threat to Personal Data: Key Factors Behind the 2023 Increase." *Apple*. December 2023. https://www.apple.com/newsroom/pdfs/The-Continued-Threat-to-Personal-Data-Key-Factors-Behind-the-2023-Increase.pdf.