Personal Data Protection Authority: Comparative Study between Indonesia, United Kingdom, and Malaysia

Vina Himmatus Sholikhah[1], Noering Ratu Fatheha Fauziah Sejati[2], Diyanah Shabitah [3]
[1] *Airlangga University, Indonesia*
[2] *Airlangga University, Indonesia*
[3] *Airlangga University, Indonesia*

ABSTRACT
The COVID-19 pandemic has increased the number of people connected to the internet. Based on data, internet users in Indonesia increased by 8.9% from 2018 to 73.7% (APJII, 2020). In addition, internet use is increasing in residential areas and residential areas (Kominfo, 2020). The development of Information, Communication and Technology Technology continues to progress, it needs to be accompanied by data protection regulations. However, Indonesia does not yet have a data protection regulation that can be implemented on the threat of cyber attacks. This research is aimed at finding best practices in data protection that can be applied in Indonesia. This study uses the Narrative Policy Framework (NPF). In the analysis, a comparison is made between data protection authorities to protect data in Indonesia and best practices in the UK and Malaysia, especially in post-pandemic conditions. This study aims to recommend solutions that strengthen data security protection in the post-COVID-19 era in Indonesia.

CONTACT
vina.himmatus.olikhah-2018@fkm.unair.ac.id

KEYWORDS
Data Protection Authority, Information, and Technology, Post-Pandemic Covid-19

INTRODUCTION

The Covid-19 pandemic has caused various problems, ranging from health issues to cybersecurity in Indonesia. As a matter of fact, internet technology and information are no longer a supporting system during this pandemic, however, they have become a major necessity for everyone. Social interactions, government services, and businesses rely heavily on the internet. Through the policy of the Ministry of Health of the Republic of Indonesia Number 9 of 2020 regarding Large-Scale Social Restrictions, the Government of Indonesia emphasizes that all physical activities can be carried out by maximizing online facilities. It resulted in what was initially a face-to-face meeting becoming a virtual meeting in which people can conduct a transaction or to simply meet one another virtually. This change is known as disruption. According to its definition, disruption is a change which occurs as a result of the presence of the future to the present time. Such a change makes everything which was originally running normally suddenly have to change and stop due to the existence of something new [1]. This era of disruption has made data playing a crucial role in the development of business and industry. Therefore, with good management and supervision, innovation and the digital economy in Indonesia will develop rapidly.

Today, the use of technology by Indonesian society is so massive. According to a survey by the Indonesian Internet Service Providers Association (APJII), from 2019 to the second quarter of 2020, the number of internet users in Indonesia was 196.7 million users, which is equivalent to 73.7% of the population in Indonesia. Amid the massive number of Indonesian internet users, the government is still currently drafting the Act aimed to protect the privacy of data digitally to improve cybersecurity. In the meantime, the large number of internet users in Indonesia is of course a huge potential to become the target of cyberattack and yet cybersecurity in Indonesia is very concerning. The National Cyber Security Index survey from the e-Governance Academy shows that cybersecurity in Indonesia scores 19.48 with the development of technological advances around 50.22. This means that there is a large difference (30.74) between technological advances and cybersecurity in Indonesia. As expected, there has been an increase in cyber attacks during the Covid-19 pandemic. Pursuant to BSSN's data, there are 290.3 million cyber attacks targeted to Indonesia in 2019 and this number reached a total of 495,337,202 cyberattacks in 2020 [2]. As counted from January 1 to April 12, there are 25 cyber attacks using the background of the Covid-19 pandemic issue. One of which is the offer on Covid-19 patients' data in Indonesia found on the online RaidForums, which was uploaded on June 18, 2020. The data offered includes a population identification number (NIK), name, age, gender, telephone number, as well as the results of their Covid-

10.52162/3.2021112

19 test. This problem arose because there is a complicated effort in maintaining individual privacy while complying with the need to support public health efforts during a pandemic, in which it requires global surveillance with the help of new technologies [3]. The public's need to acquire internet access during a pandemic has the consequence of being willing to register their data as a prerequisite to join and subscribe to the intended e- commerce. This makes internet security become more vulnerable and easy to be hacked, as well as misused by irresponsible individuals. Therefore, there are plenty of cases related to data leakage, such as what happened to the e-commerce Bhinneka.com and Tokopedia in 2020. Cases of hacking personal data often occur for several reasons. By citing the statement of the Expert Staff of the Minister of Communication and Informatics in the Legal Affairs of the Republic of Indonesia, Henri Subiakto, explained several reasons to hack a personal data, which are (1) to seek profit, (2) to perform data analysis (data mining), and (3) for the political interests of a group. Moreover, a cybersecurity analyst opines that the stolen personal data can be used to make online loans using other people's identity given that personal data sold freely on the black market (dark web) contains a detailed identity required to obtain a loan. In any event, the massive cases of personal data theft is prompted by the low level of public awareness of security and privacy threats [4]. According to the data, the increasingly massive practices of personal data collection by mobile applications and operating systems will exacerbate privacy concerns among application users. Concurrent with the lack of awareness of the users who upload their personal data, such as photos, phone numbers, and addresses in a device without an antivirus, their personal data become more vulnerable to being hacked or even traded. Therefore, the role of the personal data protection authority is very pivotal. The establishment of this authority is not merely a manifestation of the government's obligation to ensure the protection of personal data but also to control and supervise data from public bodies. Citing the provision of Article 4 (21) of the EU GDPR, it states that 'supervisory authority' means an independent public authority which is established by a Member State under Article 51". This provision indirectly obliges a Member country to form a "supervisory authority" whose task is to monitor and enforce regulations on personal data protection and to disseminate public awareness and understanding of the importance of risks and protection of personal data. In the midst of the many cases of personal data hacking which occurred in Indonesia, the government has not issued any provisions regulating the protection of personal data. Whereas, the protection of personal data is a form of fulfillment of human rights for all of Indonesian people as addressed in article 28G of the 1945 Constitution of the Republic of Indonesia.

Hence, the purpose of writing this article is to provide policy recommendations which can answer the problem of personal data in Indonesia. Acknowledging that the post-pandemic life is rock-solid with the field of digitization and future technology, it is imperative to conduct academic studies aimed at encouraging the drafting and legalization of cybersecurity regulation. Thus, the purpose of writing this article is to provide policy recommendations that can answer data protection problems in Indonesia in order to maintain data privacy. Considering that post-pandemic community life cannot be separated from the field of digitalization and future technology, academic studies aimed at encouraging the birth of a cybersecurity legal umbrella are very important so that the legalization process and its preparation can be accelerated and prioritized in Indonesia. Before going further, there are some assumptions that need to be known in the discussion of data protection and data privacy. In short, data protection is about securing data from unauthorized access. Whereas data privacy is about authorized access — who owns it and who defines it [5]. In this study, the focus of the discussion is on solutions for data protection in Indonesia. Discussions on data privacy are an important addition to the need for data protection regulations.

METHODS

The research method used in this research is a qualitative method with the Narrative Policy Framework (NPF) analysis. The Narrative Policy Framework is used to explore the narrative foundations of a public policy [6]. The policy in the context of this research is the Personal Data Protection Bill. This study uses meso-level analysis by comparing Indonesia with the United Kingdom (UK) and Malaysia. These countries were selected by purposive sampling technique based on certain considerations. First, the UK was chosen because it is considered a country with the best best practice in implementing data protection regulations known as GDPR. Second, Malaysia was chosen as a country that has several contexts in common with Indonesia as a developing country. Malaysia is a country in ASEAN that has best practice in implementing data protection regulations known as PDPA. This study uses a level of meso analysis by making comparisons among Indonesia and the United Kingdom as well as Malaysia by

using the table below. The sources of the unit of analysis used in this research are textual documentations, either from policy documents, related news reports, as well as the previous research.

Tabel 1. Narrative Policy Framework

Concept	Definition
Policy narratives	Consist of four element-setting, character, and moral of the story
Policy narrative element: The Setting	Consist of legal and constitutional parameters, geography, economic condition, and another factor regularly deemed relevant by policy actors involved or associated with a public policy.
Policy narrative element: Characters	Three categories of character: victims that are harmed by the problem, villains that intentionally or unintentionally cause the harm, and heroes that provide or promise relief from the harm
Policy narrative element: Moral of the Story	The policy solution promoted by a policy narrative

Source: (Gray & Jones, 2016)

The four elements above will be things that need to be compared from the three countries, this is done to avoid bias in the selection of research samples. The results of this comparison will be the subject of analysis and discussion. The results of the conducted comparisons found a gap among Indonesia and the United Kingdom as well as Malaysia, therefore a solution (moral of the story) can be used by Indonesia to improve cybersecurity, especially in the security of personal data protection.

RESULT AND DISCUSSION

Indonesia

As a matter of fact, the protection of personal data in Indonesia has not been regulated clearly and comprehensively, since it has not provided protection to the public. Such regulations, although not provided in a single instrument, are scattered by sector in several laws [7]. For instances, the following provisions have regulated matters related to personal data protection [8]:

1) Law Number 36 of 2009 concerning Health, Article 57 paragraph (1) "*Everyone has the right to confidential personal health conditions that have been disclosed to health service providers*";
2) Law Number 23 of 2006 concerning Population Administration, Article 1 point 22 related to the definition of personal data, "*Personal Data shall be certain personal data stored, maintained and the accuracy and confidentiality of which must be maintained.*". Then in Article 2 letters c and f, states that one of the rights of the population is the right to obtain protection for personal data, as well as compensation for errors in administration (Population Registration and Civil Registration) and misuse of Personal Data by the Implementing Agency. The personal data referred to are KK number, NIK, date/month/birth, information about physical and/or mental disabilities, as well as some contents of important events notes;
3) Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) as amended in Law Number 19 of 2016.

As shown above, personal data is only regulated sectorally in each sector, thus it does not guarantee the protection of personal data as a whole and comprehensively. Apart from the aforementioned provisions, another instrument regulating personal data protection is the the Regulation of the Minister of Communication and Information of the Republic of Indonesia Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems. In its article (1) number 1 and 2, personal data is defined as any true and tangible personal data which are inherent and identifiable to a person, specific individual data which is stored, maintained, and maintained for the truth and protected by its confidentiality. This

provision also includes protection against the acquisition, collection, processing, analysis, storage, appearance, announcement, transmission, distribution, and destruction of personal data. The authority to supervise and resolve personal data disputes under these provisions is the authority of the Directorate General of Aptika Kominfo. The Directorate General of Aptika Kominfo is one of the director generals in the field of informatics applications which is structurally under the Ministry of Communication and Information. The protection of personal data by Kominfo takes the form of preventive and repressive forms. In the preventive efforts, the authority of Kominfo is to ensure the security of the Electronic System Provider (PSE) server through certification (Article 5 paragraph 1 Regulation of the Minister of Communication and Information of the Republic of Indonesia No. 20 of 2016 (Permenkominfo No. 20/2016). When verified, PSE is obliged to send report evaluations to the Directorate General of Aptika to be used as evaluation and supervision in the form of an audit trail record to determine whether there's an indication of violations of personal data protection (Article 22 paragraph (1) Government Regulation concerning Electronic Systems and Transactions Operation). If there is a monitoring mechanism for personal data protection where the minister can request PSE information and data periodically if needed (Article 35 Permenkominfo No. 20/2016). Meanwhile, in repressive measures, any data owner or PSE operator can file a complaint with the minister if there is a failure to protect personal data. To be able to resolve disputes through deliberation and if no consensus is reached, a dispute resolution panel can be formed. (Articles 29-30 Permenkominfo No. 20/2016). The good performance of the Directorate General of Aptika is proven by the investigation of cases related to the leakage of KPU (General Election Commission) personal data in 2020, in its implementation, Kominfo has coordinated with the KPU and BSSN (National Cyber and Crypto Agency). As a result, the data found is an open data to achieve public transparency as obliged by statutory regulations. The data discrepancy occurred based on the narrative of the Indonesian KPU Commissioner Viryan, a claim for personal data leakage was 230 million DPT (Permanent Voter Data), while the existing data during that year was only 190 million[9]. Even though the Minister of Communication and Information Technology Regulation of the Republic of Indonesia Number 20 of 2016 concerning Personal Data Protection in Electronic Systems has been in force, it is not sufficient to fulfill the right to protect people's data if merely implemented in a ministerial regulation, because the ministerial regulation cannot anticipate data exchange activities which legally occur across international border. The existence of massive technology leads to a massive data exchange. For instance, the United Kingdom has a regulation to protect the personal data and the commitment not to share the data to any other countries for any purposes, even in a lawful manner. This regulation applies to countries which do not have laws that specifically regulate the protection of personal data as they have. So, for now to overcome the leakage of personal data, the government plans to immediately complete the Personal Data Protection Bill which has been included in the Prolegnas 2021. In addition, the government is aggressively conducting socialization of personal data protection through socialization of webinars and other offline socializations.

United Kingdom

The United Kingdom is a country with a fairly decent personal data protection system, it is ranked 18th out of 160 countries based on a recent survey by the National Cyber Security Index. Awareness of the importance of the legal umbrella for the protection of personal data has existed since 2013 in UN resolution 68/167 on the Right to Privacy in the Digital Age. Eventually, the legal umbrella was completed in 2016, known as the European Union-General Data Protection Regulation (EU-GDPR). It was effectively implemented in May 2018. This GDPR policy has been widely adopted by various countries as an example of best practice in making personal data protection policies [10]. The implementation of GDPR policies in Europe which has been running effectively is followed in parallel by various countries. This is conducted to fulfill a certain standard of data protection in order to exchange data between countries. One of the successful mechanisms in implementing personal data protection is the regulation regarding the authority to oversee data confidentiality as an independent commission. The commission, namely, the Data Protection Authority (DPA) is an independent public authority to oversee, investigate and has corrective powers on the application of the GDPR. The DPA also has a task to provide expert advice on data protection issues, handle complaints filed against violations of the GDPR and relevant national laws, namely, in Chapter VII Sections 68 - 76 [11]. To be able to work effectively and can be implemented consistently, GDPR requires the collaboration of all stakeholders, including DPA or data protection authorities from each state, controllers, processors, data subjects, and the European Commission, namely, European Data Protection Board (EDPB).

In the context of personal data protection in the UK, they have the UK-GDPR, a set of policies which are especially contextualized. It is known as the Data Protection Act 2018 as the UK's implementation of the general data protection regulation (GDPR). The Data Protection Act 2018 controls how personal information is used by organizations, businesses or the government. Everyone responsible for using personal data has to comply with strict rules called 'data protection principles'. They must make sure the information is: (1) used fairly, lawfully, and transparently; (2) used for specified, explicit purposes; (3) used in a way that is adequate, relevant, and limited to only what is necessary; (4) accurate and, where necessary, kept up to date; (5) kept for no longer than is necessary; (6) handled in a way that ensures appropriate security, including protection against unlawful or unauthorized processing, access, loss, destruction or damage [12]. There is stronger legal protection for more sensitive information, such as; race, ethnic background, political opinions, religious beliefs, trade union membership, genetics, bio-metrics (where used for identification), health, sex life, or orientation. There are separate safeguards for personal data relating to criminal convictions and offenses. Under the Data Protection Act 2018, subjects have the right to find out what information the government and other organizations store about them. These include the right to; (1) be informed about how their data is being used; (2) access personal data; (3) have incorrect data updated; (4) have data erased; (5) stop or restrict the processing of the data; (6) data portability (allowing them to get and reuse their data for different services); (7) object to how their data is processed in certain circumstances. Subjects also have the rights when an organization uses their data for automated decision-making processes (without human involvement) profiling, for example, predicting their behavior or interests (Data protection, nd)., In this case, the data processor and controller have supervisors. The data monitoring agency in the United Kingdom is known as the ICO (Information Commissioner's Office). The ICO has the power to take action against controllers and processors under the UK GDPR. The UK's independent authority to set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals (Controllers and processors, nd). ICO in this case has a task to receive reports of misuse of personal data and to follow up with the authorities, making up-to-date research for effective and efficient solutions in the protection of personal data, as well as being a representative on the European data protection commission.

Evidence of ICO's works can be seen in the 2016 Facebook user data leakage case used for campaign purposes. In 2018, through an ICO investigation, it was found that Facebook has used tens of millions of user data around the world for the benefit of the two parties' campaign in the UK referendum leaving the European Union (Brexit) in 2016, in this case Facebook is considered to have failed in protecting its user data. Therefore, based on data protection regulations in the UK, the ICO will fine Facebook for US $660,000 or the equivalent of Rp9.4 billion [13].

Malaysia

Malaysia has had regulations regarding the protection of personal data since 1998, namely the Communications and Multimedia Act 1998. The target of the 10th policy stipulated in the 1998 CMA, which are ensuring information security, and reliability & network integrity resulted in the Personal Data Protection Act 2010 which was in effect since 2013. With the existence of this Act, Malaysia has an agency which oversees the processing of personal data of individuals involved in commercial transactions with User Data so that it is not misused by related parties, namely the Personal Data Protection Department (PDPD), an agency under the Ministry of Communications and Multimedia Commission (MCMC). It was established on May 16, 2011 [14]. In enforcing the PDPA, commissioners are also mandated to register all classes of data users under the Order. The Commissioner has the power to carry out inspections of the data protection system under the PDPA. The 2013 regulation also stipulates that personal data systems must be open to inspection by commissioners or inspection officers at appropriate times. During these inspections, documents such as consent and notification forms can be requested. In addition, a list of third-party disclosures or other documentation proving compliance with the standards issued by the commissioners will also be requested by the commissioners. Commissioners also have the authority to appoint data user forums, issue and register codes of practice, carry out investigations into the receipt of complaints, serve law enforcement notifications, and authorize officers to take law enforcement action. Malaysia also has five additional laws addressing the appointment of a Commissioner for Personal Data Protection, registration of data users, and any fees that may be incurred. These additional legislation were passed simultaneously to facilitate the enforcement of the PDPA. The laws which have been passed to date include[15]; (1) the Personal Data Protection Regulations 2013 ('the 2013 Regulations'); (2) the Personal Data Protection (Class of Data Users) Order 2013 ('the Order'); (3) the Personal Data Protection

(Registration of Data User) Regulations 2013 ('Registration Regulation'); (4) the Personal Data Protection (Fees) Regulations 2013; (5) the Personal Data Protection (Compounding of Offences) Regulations 2016 ('Compounding of Offences Regulations'); and (6) the Personal Data Protection (Class of Data Users) (Amendment) Order 2016 ('the Order Amendment'). In carrying out personal data protection, several related parties are interconnected. The parties involved in personal data protection in Malaysia include a) User data as individuals or groups who process any personal data or have control / permit the processing of any personal data, such as Maybank, Malaysia Airlines, POS Malaysia, Celcom, BIG; b) data processor is any person who processes personal data only on the name of the data user and does not process personal data for their purposes, such as vendors, dealers; c) Subject data, namely each individual as the subject of personal data, for example, students, patients, employees, citizens, and non-citizens.

The existence of a supervisory agency and regulations for the protection of personal data in Malaysia, in fact, still has a gap in the occurrence of cyber attacks. Based on the data from the Malaysia Computer Emergency Response Team, the total number of Malaysia's computer security incidents from January to April 2021 is 3,647. The incident consisted of 141 cyber harassment, 30 spams, 7 denials of services, 173 malicious code, 49 Intrusion Attempts, 2540 frauds, 29 Contents Related, 649 Intrusions, and 29 Vulnerability reports [16]. Back in 2020, between January and October 2020, Malaysia experienced a Macau Scam of 5,218 cases, causing a loss of more than 256 million Malaysian Ringgit (MYR). The Macau scam is a fraud in which it leads the victims to give large amounts of money through telecommunications connections, the scam perpetrators are not only local but also international, especially from Hong Kong [17].

Tabel 2. Narrative Policy Framework Indonesia, Malaysia, United Kingdom

Concept	Indonesia	United Kingdom	Malaysia
Policy narratives	-	UK - GDPR and DPA 2018	Personal Data Protection Act 2010
Policy narrative element: The Setting	- Provisions for the protection of personal data are contained in several sectoral regulations (ITE Act, Permenkominfo, Health Act, and Population Administration Act) - Kominfo issues Permenkominfo which regulates data protection comprehensively, but the legal force is weaker than an Act (through Ditjen Aptika and BSSN)	- Endorsement and completion of the EU-GDPR in 2016. Effective implementation in May 2018. - The parties involved are DPA as well as data protection authorities from each state, controllers, processors, data subjects, and the European Commission namely, the European Data Protection Board (EDPB)	- Communications and Multimedia Act 1998 Regulation regarding the protection of personal data since 1998 - Personal Data Protection Act 2010 in effect since 2013 - Personal Data Protection Department (PDPD), an institution under the Ministry of Communications and Multimedia Commission (MCMC) which was founded on May 16, 2011

Policy narrative element: The Setting	- Provisions for the protection of personal data are contained in several sectoral regulations (ITE Act, Permenkominfo, Health Act, and Population Administration Act) - Kominfo issues Permenkominfo which regulates data protection comprehensively, but the legal force is weaker than an Act (through Ditjen Aptika and BSSN)	- Endorsement and completion of the EU-GDPR in 2016. Effective implementation in May 2018. - The parties involved are DPA as well as data protection authorities from each state, controllers, processors, data subjects, and the European Commission namely, the European Data Protection Board (EDPB)	- Communications and Multimedia Act 1998 Regulation regarding the protection of personal data since 1998 - Personal Data Protection Act 2010 in effect since 2013 - Personal Data Protection Department (PDPD), an institution under the Ministry of Communications and Multimedia Commission (MCMC) which was founded on May 16, 2011
Policy narrative element: Characters	**Heroes:** - Kominfo - BSSN - Other ministries **Villain:** - Cyber Attack (data leak) - Arrangements that are still sectoral - PDP provisions are regulated only in Permenkominfo, not an Act **Victim:** - Security of citizens' Cyber Attack data - Security of private personal data (business entities) - Government data security (public bodies)	**Heroes:** - ICO and EPDB **Villain:** - Cyber attack **Victim:** - Security of citizens' personal data - Security of personal data from industry players	**Heroes:** - PDPD **Villain:** - Cyberattack - Personal data security regulations only in the commercial field **Victim:** - Security of citizens' data - public field data security
Policy narrative element: Moral of the Story	Data protection arrangements in Indonesia are only regulated by sector. Thus, law enforcement has not been maximal and has not provided legal protection for the community.	UK-GDPR to protect people's data can work well with the collaboration of various parties and the role of ICO as an independent data monitoring agency.	PDPA only protects the security of personal data in the commercial field

Source: Author

Regardless of the table above, it can be seen that Indonesia still does not have any legal regulations regarding the protection of personal data, while the United Kingdom has UK-GDPR and DPA 2018; and Malaysia has PDPA 2010. The setting of the policy narrative in Indonesia exists in several sectoral regulations, whereas the United Kingdom and Malaysia have integrated regulations to regulate personal data. Nevertheless, Indonesia has some heroes of the policy narrative element, such as BSSN, Kominfo, and other ministries. Meanwhile, in the UK it has an ICO and EPDB; and Malaysia has a Personal Data Protection Department. These three countries have the same villain, namely cyber attacks. It can be concluded that even though a country has decent and integrated regulations, there is still a risk of cyber attacks. Besides that, the victims of the policy narrative elements of the three countries have the same cases, such as public data protection and citizen data protection. At least, from the discussion above, the moral of the story from Indonesia is regulation of data protection in Indonesia is only regulated by sector. Thus, law enforcement has not been implemented maximally and has not provided legal protection for the citizen. From the United Kingdom, we can take the value that UK-GDPR protects people's data decently with collaboration from various parties and the role of ICO as an independent data monitoring agency. Malaysia gives the moral value that their actions only protect the personal data of the commercial sector. Thus, it appears that Indonesia has quite a fundamental weakness and considerable implications for the enforcement of personal data protection. This weakness is evidenced by the absence of comprehensive provisions relating to the protection of personal data. This has resulted in massive cases of leakage of personal data in Indonesia which are increasingly causing worries in the community. This is due to the separate sectoral regulations which are included in at least 32 Acts, such as the Population Administration Act, ITE Act, Health Act, and other acts and regulations. However, if we look at the reality, cases of cyber attacks and leaks of personal data are very complex and require law enforcement which involves all parties. The absence of a law specifically regulating personal data is the main reason why the personal data regulation has not been harmonized in several regulations. The Personal Data Protection Bill (RUU) that will be passed later, at least regulates the balance of rights and obligations between data users and data controllers. Moreover, the Personal Data Protection Bill will have to explicitly regulate the supervisory agency assigned and authorized to have the authority to resolve and provide policies on personal data protection in order to diminish the potential for abuse of authority.

Based on the NPF analysis comparing the United Kingdom, Malaysia, and Indonesia, it can be said that Indonesia needs an independent data monitoring agency so that the regulations that have been set can be implemented effectively. This is because independent data monitoring agencies are an important aspect of protecting people's data [18]. So that data protection regulations in Indonesia need to explicitly regulate the legal basis that establishes the mandate, powers, and independence of these authorities. In general, there are two models for the formation of an independent supervisory agency, namely, the creation of an independent supervisory authority, and the two models based on ministries [18]. The best practice form from an independent supervisory authority exists in the United Kingdom's ICO. Meanwhile, the ministerial-based supervisory agency can see Malaysia's PDPA practice. Through a comparison between the two data monitoring agencies, the authors conclude that a supervisory agency with an independent authority outside the state-owned ministry base can effectively reduce data fraud practices in the private and public sectors.

In addition, if you understand their duties and roles, independent institutions need to ensure that personal data protection regulations are complied by data controllers and processors, either individuals, the private sector, or public institutions. Thus, the role of independent institutions is not only in implementing policies, but also in terms of increasing public awareness of data protection, serving consultation on reports of victims of abuse of personal data, and developing networks for collaboration in maintaining data security. In this case, the authors recommend that an independent supervisory body be formed such as the ICO belonging to the United Kingdom. Because it is expected that the supervisory agency is not only assigned to oversee the private or private sector, such as business companies, etc, but can also supervise government institutions with public authorities such as the executive, legislative, and judiciary bodies. A supervisory agency such as an ICO is created in the form of a commission because it is not directly governed by the constitution, however, the importance of establishing an institution, in this case, the Data Protection Authority has been regulated under the GDPR. The independent institution that we refer to in this case is what is also regulated under the criteria for an independent institution in article 52 of the EU GDPR [19], which include; (1) Institutionally independent; (2) Independent of Human Resources; (3) Organizationally independent; (4) Independent from Financial Control. To reaffirm our stance, in ensuring the security of personal data, there needs to be a role from an independent supervisory

agency which must be regulated under a specific Act in order for the agency to have a legal power as state auxiliaries which are not co-opted by the dominance of executive and legislative powers.

CONCLUSION

Along with the massive number of internet users in Indonesia during the Covid-19 pandemic, the potential for cyber attack cases can also arise, moreover, Indonesia does not have a regulation or a personal data security supervisory authority. This has contributed to the increasing vulnerability in personal data security during the Covid-19 pandemic which demands everything to use technology and mandatory filing of personal data. On the other hand, leakage of personal data occurs not only in the private sector but also in the public sector, such as in the case of the disclosure of health data for Covid-19 patients. The results of the analysis using the NPF method by comparing the United Kingdom, Malaysia, and Indonesia, it is found that the hero characters in Indonesia still do not have integrated regulations governing the protection of personal data, while UK and Malaysia have had these regulations for a long time. This has resulted in villains or threats of crimes such as cyber attacks. These three countries have the same victims, namely public data protection and citizen data protection. Therefore, in ensuring the security of personal data in Indonesia, apart from hastening the enforcement of the PDP Bill which is being formulated firmly. The authority and duties of an independent supervisory agency in the form of a commission must be regulated under a specific Act in order for the agency to have a legal power as state auxiliaries which are not co-opted by the dominance of executive and legislative powers.

REFERENCE

[1] Kasali R. Self Driving. 1st ed. Jakarta Selatan: Mizan; 2018.
[2] Anjani N. Perlindungan Keamanan Siber di Indonesia [Internet]. Id.cips-indonesia.org. 2021 [cited 15 May 2021]. Available from: https://id.cips-indonesia.org/post/ringkasan-kebijakan-perlindungan- keamanan-siber-di-indonesia
[3] Revilia, D., & Irwansyah, N. (2020). Social Media Literacy: Millenial's Perspective of Security and Privacy Awareness. Jurnal Penelitian Komunikasi Dan Opini Publik, 24(1).
[4] Xu, H., Gupta, S., Rosson, M.B., Carroll, J.M., 2012. Measuring Mobile Users' Concerns for Information Privacy. Thirty Third International Conference on Information Systems, Orlando [5] Wicaksana, R., Munandar, A. and Samputra, P., 2020. A Nar r ative Policy Framework Analysis of Data Privacy Policy: A Case of Cyber Attacks During the Covid 19 Pandemic. [online] Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi). Available at: <http://dx.doi.org/10.33164/iptekkom.22.2.2020.143-158> [Accessed 1 May 2021].
[5] Robinson, R., 2020. Data Privacy vs. Data Protection. [online] Blog.ipswitch.com. Available at: <https://blog.ipswitch.com/data-privacy-vs-data-protection> [Accessed 12 June 2021].
[6] Fischer F, Forester J. The Argumentative turn in policy analysis and planning. Durham: Duke University Press; 2005.
[7] Yuniarti, S. (2019). Perlindungan Hukum Data Pribadi Di Indonesia. Business Economic, Communication, and Social Sciences (BECOSS) Journal, 1(1), 147-154.
[8] Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. Jurnal Cakrawala Hukum, 10(2), 218-227.
[9] Dwi Andayani, 2020, https://news.detik.com/berita/d-5024304/jutaan-data-diduga-bocor-kpu-dpt- 2014-bersifat-terbuka
[10] Wahyudi Djafar dan M. Jodi Santoso, 2020, 'Perlindungan Data Pribadi: Pentingnya Otoritas Pengawasan Independen'. https://elsam.or.id/perlindungan-data-pribadi-perlunya-otoritas-pengawasan-independen/ accessed 25 Mei 2021.
[11] Arbella W. Perbandingan Hukum Terhadap Perlindungan Data Pribadi Menurut Hukum Positif Indonesia Dan General Data Protection Regulation (Gdpr) Uni Eropa Skripsi [Bachelor]. Universitas Sumatera Utara; 2020.
[12] GOV.UK. n.d. Data protection. [online] Available at: <https://www.gov.uk/data-protection> [Accessed 23 May 2021].
[13] Natalia, E., 2018. Kasus Data Bocor, Inggris Akan Denda Facebook Rp 9,4 M. [online] CNBCnews. Available at: <https://www.cnbcindonesia.com/news/20180711135404-4-23036/kasus-data-bocor- inggris-akan-denda-facebook-rp-94-m> [Accessed 23 May 2021].
[14] Mazmalek bin Mohamed Director General Personal Data Protection Department Ministry of Communications & Multimedia. 20XX. Personal Data Protection Law in Malaysia was accessed on

23 May 2021 by https://www.pdp.gov.my/jpdpv2/assets/2020/01/Introduction-to-Personal-Data-Protection-in-Malaysia.pdf

[15] Ping, JCY., DataGuidance. 2021. Malaysia - Data Protection Overview. [online] Available at:<https://www.dataguidance.com/notes/malaysia-data-protection-overview> [Accessed 30 May 2021].

[16] Malaysia Computer Emergency Response Team. 2021. Reported incidents based on general incidents classification statistics2021 was accessed on 23 May 2021 by https://www.mycert.org.my/portal/statistics-content?menu=b75e037d-6ee3-4d11-8169- 66677d694932&id=be86863d-8027-4379-99d5-40861090b502

[17] Interpol. 2021. Asean Cyberthreat Assessment 2021 Key Cyberthreat Trends Outlook From The Asean Cybercrime Operations Desk

[18] Nurtjahjo H. Lembaga, Badan, Dan Komisi Negara Independen (State Auxiliary Agencies) Di Indonesia: Tinjauan Hukum Tata Negara. Jurnal Hukum dan Pembangunan Tahun-35 No 3. 2005;:275- 287.

[19] General Data Protection Regulation (GDPR) – Official Legal Text [Internet]. General Data Protection Regulation (GDPR). [cited 1 May 2021]. Available from: https://gdpr-info.eu/