UUM JOURNAL OF LEGAL STUDIES
https://e-journal.uum.edu.my/index.php/jls

How to cite this article:
Faiz Rahman. (2025). Safeguarding personal data in the public sector: Unveiling the impact of the new personal data protection act in Indonesia. *UUM Journal of Legal Studies*, *16*(1), 1-18. https://doi.org/10.32890/uumjls2025.16.1.1

SAFEGUARDING PERSONAL DATA IN THE PUBLIC SECTOR: UNVEILING THE IMPACT OF THE NEW PERSONAL DATA PROTECTION ACT IN INDONESIA

Faiz Rahman
Leiden Law School, Universiteit Leiden, the Netherland
Faculty of Law, Universitas Gadjah Mada, Indonesia

f.rahman@law.leidenuniv.nl

Received:11/7/2023 Revised: 13/5/2024 Accepted: 9/6/2024 Published: 31/1/2025

ABSTRACT

Personal data protection is a significant issue that has attracted public attention in recent years due to various personal data leaks, especially those held by public sector institutions. The issue prompted lawmakers to re-open the discussion of the Personal Data Protection Bill (PDP Bill), which was finally enacted in October 2022. An essential aspect addressed in the newly enacted PDP Act was data protection by public sector institutions in Indonesia. Several studies showed that the collection of personal data by these institutions is primarily mandatory. Therefore, this study examines the laws and regulations related to personal data protection by public sector institutions and the potential implementation challenges. The challenges include the tendency to "prioritise" sectoral regulations over the PDP Act and the potential to "over-utilise" and "over-interpret" data protection exemptions. The findings indicated that the newly enacted PDP Act provided excessive leeway for public institutions to exempt data subjects' rights despite the high standard for data processing. The findings suggested that to achieve a meaningful implementation of the PDP Act, the mandated supervisory authority must be independent in carrying out its duties and functions to ensure the just enforcement of personal data protection in the public and private sectors. In addition, the government must develop a strategy to ensure the consistency of data protection implementation through various legislations currently being drafted, as well as harmonising the PDP Act with other related Acts.

Keywords: Data protection, legal framework, personal data protection Act, public sector, supervisory authority.

INTRODUCTION

The digitalisation of the public sector has been conducted to improve the quality and accessibility of various public services (Kuziemski & Misuraca, 2020; Rumbold & Pierscionek, 2018). Although this transition offers advantages for both the government and the public, it also presents significant challenges concerning data protection (Alsenoy et al., 2011; Chik, 2013; Fuster, 2014). In Indonesia, there has been a considerable increase in data breach incidents within the public sector, specifically during the COVID-19 pandemic and post-pandemic periods when many government services shifted to online platforms. According to the Ministry of Communication and Informatics (2023), there were 98 cases of data breaches from 2019-2023 in both the private and public sectors. The unforeseen circumstances caused by the COVID-19 pandemic compelled the Indonesian government to expedite the development of digital services for administrative and public service purposes, recognising the impossibility of halting operations (Agostino et al., 2020). Consequently, the Indonesian government is unavoidably confronting various challenges, including data breaches and privacy concerns.

Several incidents have captured public attention, particularly the National Health Social Security Agency and electronic Health Alert Card (eHAC) data leak in mid-2021 (BBC Indonesia, 2021; Galuh, 2021), alongside the General Election Commission's leak of voter data and COVID-19 patient data leak in 2020 (CNN Indonesia, 2020; Fahmi, 2020). These breaches were associated with population administration data, comprising citizen identification numbers, family card numbers, dates of birth, and other types of data held by various public and private sector institutions. The incidents vividly illustrate the tangible consequences of inadequate data protection and privacy measures within the context of public sector digitalisation. As the government continues to advance the Electronic-Based Government System (E-Government), which promotes the collection and use of extensive data across various governmental services, safeguarding personal data collected by these institutions becomes essential in upholding citizens' rights to their personal data.

According to previous reports, data collection by public sector institutions adheres to established laws and regulations and is largely compulsory (Blume & Svanberg, 2013). Consequently, individuals often have limited freedom of choice regarding the disclosure of personal data compared to others in the private sector (Blume, 2015). In instances of misuse or unlawful processing, the repercussions extend beyond the authorities overseeing citizens' data to affect the broader public (Black & Stevens, 2013). Given the nature of data collection within the public sector, it is reasonable to assert that the data protection concept initially emerged from this domain (Blume, 2004).

In recent years, the increase in data breaches and misuse incidents has led various groups to call for the prompt enactment of the Personal Data Protection Bill (PDP Bill) by the House of Representatives (DPR). Despite repeated delays in discussions, the Bill was eventually finalised in September 2022 and enacted in October 2022 as Law No. 27/2022, commonly known as the PDP Act. However, it is also worth noting that regulations concerning personal data in Indonesia have been implicitly present since the 1990s. These regulations have predominantly been sector specific. For example, the Banking Act (Law No. 7/1992 jo. Law No. 10/1998) has regulated the obligation of banks to keep customers' information and deposits confidential unless otherwise stipulated by the Act (See Article 40 of the Banking Act).

Several provisions within various Acts also govern personal data, including the Population Administration Act (Law No. 23/2006 jo. Law No. 24/2013), the Electronic Information and Transactions Act or EIT (Law No. 11/2008 jo. Law No. 19/2016), Public Information Disclosure Act

or PID Act (Law No. 14/2008), and the Health Act (Law No. 17/2023). Over the years, various types of data, such as banking, health, and population administration records, have been recognised as personal data (Walters et al., 2019). Therefore, the recently enacted PDP Act assumes significance in harmonising disparate data protection frameworks across different sectors. In scrutinising the dynamics of the data protection legal framework, this study shows that the implementation of the PDP Act must prioritise public sector institutions, given the obligatory nature of data collection and use in this domain. Transparent and reliable data processing can also increase public trust in data processing by public sector institutions.

METHODOLOGY

This study has examined personal data protection in the public sector in Indonesia before and after the enactment of the PDP Act in 2022. In addition, the aim was to understand the implications of such changes and the challenges that could be faced in the implementation of the PDP Act. The insights of this study were based on the doctrinal research which examined primary and secondary legal sources (Bhat, 2019). The primary sources mainly covered Acts and regulations related to personal data protection, while secondary sources comprised journals and books discussing the subject. The primary and secondary sources were critically and systematically examined and assessed using content analysis.

Personal Data Processing in the Public Sector

The interests of the state often conflict with that of individuals, especially in protecting the latter's rights over sharing personal data. In this regard, Sloot (2017) stated that because all processed data consisted of private and public data, citizens could not decide whether to disclose their data, and the government needed such data primarily to develop policies on public services. Moreover, personal data use was essential for achieving national goals. This is because ideally, the government collected and used data as a necessity for managing social welfare and realising law and order (Regan, 1986).

The potential of massive data collection was also apparent in the digital government context, where many government institutions used numerous applications to collect and use citizens' personal data. One of the common issues in digital government studies included privacy and data protection (Brown et al., 2014; Lin et al., 2021; Muñoz & Bolívar, 2018; Otjacques et al., 2007; Thompson et al., 2015). In addition, it was logical considering the nature of digital services, which were linked to the broader internet (Thompson et al., 2020). Moreover, van Zoonen (2016) stated that collecting personal data with the aim of it being used for public services had privacy challenges, although these challenges tend to be moderate. Apart from the fact that data collection had become part of the management of public services, citizens would also obtain balanced reciprocity in their being offered public services. This was slightly different from collecting personal data used for surveillance, for example data managed by institutions such as the police, which tended to have higher privacy challenges (van Zoonen, 2016). In surveillance, data collected could be enormous and in-depth, exceeding what was originally intended. In addition, the people who were the object of surveillance often did not know the reason for their being watched (Solove, 2008).

The awareness that authorities could easily violate privacy and still always strive to continue to collect and manage data, serves as the critical context for the development of measures aimed at protecting personal data in the public sector (Hert & Gutwirth, 2006). This could be seen from the characteristics of data collection in the public sector, which was mostly carried out mandatorily based on obligations

stipulated in the provisions of the law (Blume, 2012). For instance, in collecting and using personal data for population administration, the government recorded "general" personal data, such as one's date of birth and address, and more sensitive or "special" data, including biometrics. Considering the state's "power" to oblige citizens to provide their data to government institutions, it was logical that fairness and reasonableness of processing had become an essential part of data protection principles (Sloot, 2017). It is deemed that such measures will minimise the potential abuse of government power in its management of citizens' data held by government agencies.

In recent years, widespread digitalisation, particularly in the public sector, has significantly increased the use of personal data to support operational processes. This indicated the importance of these data in contemporary settings. In this digital era, every activity, including government, often depends on data. Consequently, the government must assess and evaluate data to ensure that policymaking is based on the factual data collected, and not on any other considerations. This showed that more data (including personal data) needed to be continuously collected, stored, and managed (Xiao, 2019). For instance, the OECD reported in 2020 that various entities had increased personal data use for economic and social purposes. These included internet service providers, online sales, financial service providers, and the Government (OECD, 2020). Therefore, various public sector entities collected and managed different personal data according to their respective needs. Although the data collected was diverse, each public sector institution had the same obligation to protect the data collected (Thompson et al., 2015).

Technological advancement and complexity in this digital era have progressively increased the awareness of personal data protection. Government institutions now utilise more sophisticated technologies to collect, analyse, use, and conduct surveillance (Rubinstein et al., 2014; Wu, 2014). This shift in emphasis has been consistent with the argument that the institutional power to collect data and technological development have significantly influenced the practice of collecting and processing personal data, which would have an impact on the decreased level of personal data protection from other party access (Keller, 2019). Awareness of personal data protection must be reflected in the timely necessary provision of guarantees or security standards by public sector institutions. In addition, it has also emphasised the urgent need to examine the appropriate regulation that will foster a true understanding of the importance of compliance with privacy rights in the technological development era (Wu, 2014). The government's application of personal data protection is also aimed at unifying the fundamental conflict between privacy, the freedom of information, and the need for data to carry out governance (Hert & Gutwirth, 2006). Data collection by public sector institutions was often carried out mandatorily, showing that individuals lacked the freedom to choose whether to disclose their data (Blume, 2015). Therefore, more robust data protection could reduce power and information asymmetries, which caused the relationship between data subjects and data controllers to become imbalanced (Lynskey, 2014). Laws and regulations also significantly balanced (or at least proportionately) the "imbalanced" relations between the state and citizens in personal data use.

The implementation of personal data protection in the public sector must also be examined from a human rights point of view. In addition, several studies have demonstrated the interconnectedness of privacy and data protection (Kokott & Sobotta, 2013). However, data protection has been essential in actualising the protection of the right to privacy, specifically informational privacy, considering the threat to privacy in the age of digital technologies, where personal data have been more accessible and potentially prone to misuse. Previous reports also showed the inclusion of personal data protection as part of human rights (Yu & Zhao, 2019). Therefore, the state needed to provide an appropriate method of protection for these rights through the availability of unique content (Xiao, 2019). This must be included as part of the state's responsibility to respect, protect, and fulfil citizens' rights. In Indonesia,

the state's obligations to protect, promote, enforce, and fulfil human rights are stated in the Constitution.[1]

Public Sector Data Protection before the PDP Act 2022: Sectionalism and its Implications

Although the constitutional basis of the right to data protection is still a discourse among Indonesian scholars, the majority had agreed that it was part of the protection of the right to privacy (Rahman & Wicaksono, 2021). In the 1945 Constitution of the Republic of Indonesia (henceforth, the 1945 Constitution), the right to privacy was often associated with Article 28G paragraph (1), specifically regarding the "protection of oneself." The Electronic Information and Transactions Act (EIT Act) explicitly mentioned the relationship between data protection and the right to privacy in the Elucidation of Article 26 paragraph (1). In addition, Article 26 of the EIT Act was the only article in the EIT Act that regulated personal data, specifically on the need for consent in using personal data.

Another Act that was also fundamental in protecting privacy in Indonesia was the Human Rights Act (Law No. 39/1999). Although the term "privacy" was not explicitly used, the protection of privacy could be seen in several Articles as part of the right to individual freedom (See Articles 20 to 27) and the right to security (Articles 28 to 35). For instance, concerning data protection, Article 21 of the Human Rights Act stated that a person could not be an object of research without their approval, which was essentially related to the need for consent. Another example is Article 32, which stated that a person has freedom and confidentiality in correspondence, including communication through electronic media.

Based on the explanation above, the Indonesian legal framework considered personal data protection as part of privacy rights. In addition, it was closely related to the development of personal data protection, which was inseparable from the right to privacy (Blume, 2012; Boehme-Neßler, 2016; Holvast, 2008; Regan, 1986). As the right to privacy was not absolute, it could be limited and legally "invaded" based on the law (Gavison, 1980). This showed that the limitation of the enjoyment of the right to privacy must have a solid legal basis. Article 28J paragraph (2) of the 1945 Constitution explained that the limitation of the enjoyment of human rights could only be done in accordance with Acts and comply with just demands based on the considerations for morality, religious values, security, and public order in a democratic society. Therefore, the limitation of the enjoyment of human rights must be carried out through the Act, or such a restriction would become unconstitutional. The regulation of personal data by the Indonesian Acts will determine how robust legal protection was provided with respect to personal data.

Prior to the enactment of the PDP Act, personal data was regulated by various laws and regulations in different hierarchies. According to Article 7 paragraph (1) of Legislation Act (Law No. 12/2011 *jo.* Law No. 15/2019 *jo.* Law No. 13/2022), Indonesian laws and regulations have a clear hierarchy, starting with the 1945 Constitution, MPR Decree, Acts, Government Regulations, Presidential Regulations, and Regional Regulations. Moreover, Article 8 of the Legislation Act also acknowledged various laws and regulations enacted by various state and government institutions, despite no specific position in Article 7's hierarchy of legislation.

[1] It should be noted that the 1945 Constitution of the Republic of Indonesia does not have a specific article concerning personal data protection. Nevertheless, the PDP Act refers to Article 28G paragraph (1) and Article 28H paragraph (4), which is related to the protection of personal rights and property rights. Many scholars in Indonesia refer, specifically, to Article 28G paragraph (1) as the constitutional basis for the right to privacy.

Based on the mapping and examination of Indonesian laws and regulations, there were at least 25 Acts regulating personal data in specific public sectors before the enactment of the PDP Act, and more at the national level tasked with implementing legislation (from Government Regulation to institutional regulation). Personal data which were regulated varied from banking, health, and population administration data. Various Acts regulating personal data before the PDP Act at least had a provision regarding the obligation of "data controller" and "data processor" (although using different terms according to the subject regulated in each sector) to ensure confidentiality. However, the term used for the regulated data was not always "personal data." The terms used were based on a specific sector, such as customer information in the banking sector, patient data in health, and population data in population administration. Previously, the definition of personal data at the Act level could be found only in the Population Administration Act. Article 1 of the Population Administration Act, which defined personal data as "certain individual data that stored, maintained, kept its accuracy and protected its confidentiality."

Apart from several Acts that specified "personal data" regulated in the Act, some Acts used the term "personal data," such as the EIT Act and Archive Act (Law No. 43/2009). However, these Acts did not define or explain the meaning of the term. As mentioned above, the EIT Act also had a provision concerning consent to use personal data. The definition of personal data could only be found in its implementing regulations, namely Government Regulation 82 (Government Regulation No. 82/2012 on Electronic System and Transactions Implementation) and MCI Regulation 20 (Minister of Communication and Informatics Regulation No. 20/2016 on Personal Data Protection in Electronic Systems). The definition of personal data in the two regulations above was the same as in the Population Administration Act. In addition, the Government Regulation 82 definition of "personal data" was "changed" in Government Regulation 71 (Government Regulation No. 71/2019 on Electronic System and Transactions Implementation). The definition of "personal data" in Government Regulation 71 was the same as in the current PDP Act.

As most provisions were sector-centred, personal data protection was not standardised. Therefore, the protection of personal data in specific sectors was largely dependent on sectoral regulations. In several Acts, there were some "different degrees of protection" of personal data in the "same classification" (Rahman, 2021). For example, the Population Administration Act 2013 differentiated population data (such as Family Card number, citizen identification number, sex, and date of birth) and personal data (information on physical and/or mental disabilities, fingerprint, iris, signature, and other data elements regarding a person's ignominy). However, personal data in Article 84 paragraph (1) of the Population Administration Act 2013 was also part of the population data listed in Article 58 paragraph (2).

Article 84 paragraph (1) of the Population Administration Act 2013 could be read as a necessity to protect "certain individual data", which was protected by considerations of confidentiality. Considering that the protection of confidentiality was one of the elements of personal data definition, Article 84 paragraph (1) raised the interpretation that there was personal data of the population without the need to be protected. These comprised other "individual data" listed in Article 58 that were not classified as "personal data" in the context of Article 84. In addition, this showed the inconsistencies of personal data arrangements in the Population Administration Act. The definition of the term, which seemed to be formulated in a "simple" way, created a complex interpretation and regulatory inconsistencies.

The mentioned population data above were regulated as personal data in other countries. For example, Article 2 Paragraph (1) of the Act on the Protection of Personal Information 2003 (Japan), Article 2 Paragraph 1 of the Personal Information Protection Act 2011 (Korea), and Article 4 Paragraph (1) of

EU General Data Protection Regulation (GDPR). Therefore, apart from the inconsistency of the terminology explained, the Population Administration Act also differentiated data protection for the same classification of data, which in this context is "individual data" as part of population data. Moreover, the Act also did not have a single provision concerning the protection of "population data." This showed that the Population Administration Act did not legally guarantee the protection of "population data," which conceptually and comparatively also constituted personal data. In reality, "population data" were used by many state institutions. Ironically, population administration data were the most often leaked or misused. This was evident through recent personal data (population data) leak cases, such as the Social Health Insurance Administration Body (BPJS) and Ministry of Health's electronic Health Alert Card (eHAC) case in mid-2021 and the General Election Commission (KPU) Case in 2020, as well as the Bjorka Case that led to the enactment of the PDP Act in 2022. The Ministry of Communication and Informatics (2023) noted 98 data breach cases from 2019 to 2023, which had included cases in the public sector.

Data Protection in the Public Sector Post the PDP Act 2022

The PDP Act was enacted in October 2022, but the idea of a comprehensive PDP Act was initiated way before the enactment of the Act.[2] The first published academic draft and the PDP Bill were disseminated in 2016 through the Indonesian National Laws Data and Information Network. Moreover, the Minister of Communication and Informatics (MCI) also issued the MCI Regulation 20 in 2016 to fill the legal gap in the personal data protection framework. The Indonesian government stipulated Government Regulation 71, which incorporated provisions regarding personal data protection and even provided a "new definition" of personal data. However, in practice, both regulations still could not address the sporadic and sectionalism of personal data protection framework at the Act level. This showed that the enactment of the PDP Act was intended to address the issue.

Technological advancement encouraged public sector institutions to implement more sophisticated technologies in their activities. The relationship between citizen and public sector institutions has become more uneven (See Lynskey, 2014). The collection and use of personal data by the public sector institutions were often mandatory. However, in recent years, several "big cases" concerning personal data leaks have occurred with regard to personal data held by public sector institutions. As the use of personal data was essential to manage social order and to achieve law and order, the PDP Act must also provide the necessary legal protection for the constitutional rights of citizens.

Consideration Points a and b of the PDP Act show that it is explicitly stated that personal data protection is one of the human rights considered, specifically part of the protection of oneself, and must have a solid legal basis to provide security for personal data.[3] Moreover, Consideration Point c of the PDP Act

[2] There is conflicting information regarding the year when the comprehensive PDP Bill was initiated. Some said it was in 2012 (Ministry of Communication and Informatics of the Republic of Indonesia, 2019), and others said it was way before. For example, in Graham Greenleaf's book titled "Asian Data Privacy Laws", it was mentioned that the idea to formulate a comprehensive PDP Act was prepared in 2008 under the Ministry of Administrative Reform, even though the full contents were not made public, and it had not proceeded further (Greenleaf, 2014).

[3] It is stated in Consideration Point a that "*personal data protection is one of the human rights that constitutes personal protection, therefore it is necessary to provide a legal basis to provide security for personal data, based on the 1945 Constitution of the Republic of Indonesia*." While in Consideration Point b, it is mentioned that "*that personal data protection is aimed at ensuring the right of citizens to personal protection and raising public awareness as well as ensuring recognition and respect for the importance of personal data protection*".

also admitted the sporadic regulations of personal data.[4] Accordingly, the PDP Act was expected to increase the effectiveness of the implementation of data protection through a comprehensive PDP Act. The PDP Act accommodated critical elements of personal data protection, including definition, principles, categories of personal data, the rights of data subjects and obligations of data controller and processor, and the establishment of a supervisory agency. However, several issues must be critically evaluated due to their close association with public sector data protection. The problems were mainly about the exemption in personal data processing, formulation of penalties, remedies provisions, and the establishment of an independent authority.

Exemptions of Data Subject Rights, Data Controller and Processor Obligations

The PDP Act gave a considerable number of exemptions to derogate various data subject rights and data controller and processor obligations, as is shown in Table 1 below.

Table 1

Exemption of Data Subject rights, Data Controller and Data Processor Obligations

Data Subject rights, Data Controller and Data Processor Obligations	Reasons for Exemption
Data Subject rights to end, delete, and/or destroy their personal data (Article 8); opt-out from the consent given to data controller (Article 9); objection to decision-making that is only based on automatic profiling (Article 10 par. (1)); delay or limit personal data processing proportionally (Article 11); obtain and/or use personal data regarding themselves from data controller in a form that is in accordance with the structure and/or format commonly used or readable by the electronic system (Article 13 par. (1); and use and send personal data regarding themselves to other data controllers, as long as the system can communicate securely (Article 13 par. (2)).	National defence and security; law enforcement process; public interests in the framework of government administration; supervision of financial services sector, monetary, payment system, and economic system stability; or statistical or scientific research (Article 15 par. (1))
Data Subject rights to complete, update, and/or correct errors and/or inaccuracies in their personal data (Article 6).	Endangers the security, physical health, or mental health of the person's Personal Data and/or other people; has an impact on the disclosure of other people's Personal Data; and/or is contrary to the interests of the national defence and security (Article 33)
Data controller and processor obligations to delay and limit the processing of personal data (Article 41 par (1))	There are provisions of laws and regulations that do not allow delay and restriction on Personal Data processing; it may endanger the safety of others; and/or the person's Personal Data is bound by a written agreement with Personal Data Controller which does not allow for delay and restriction on Personal Data processing (Article 41 par. (2)).

(continued)

[4] It is mentioned in Consideration Point c that "*regulations of personal data are currently contained in several laws and regulations, so to increase effectiveness in the implementation of personal data protection, it is necessary to regulate personal data protection in a law*".

Data Subject rights, Data Controller and Data Processor Obligations	Reasons for Exemption
Data controller and processor obligations to update and/or correct errors and inaccuracies in personal data and notify the changes (Article 30); provide access to personal data that is processed along with the track record of processing in accordance with the retention period (Article 32); maintain the confidentiality of personal data (Article 36); terminate personal data processing (Article 42); delete personal data in specific events (Article 43 par. (1) letter a to letter c); destroy personal data by request from data subject (Article 44 par. (1) letter b); notify data subject for deletion and/or destruction of personal data (Article 45); and notify data subject in case of failure to protect Personal Data (Article 46 par. (1) letter a)	National defence and security; law enforcement process; public interests in the framework of government administration; supervision of financial services sector, monetary, payment system, and economic system stability (Article 50 par. (1)).

Note. The contents in Table 1 are the author's explication of the PDP Act (Indonesia), 2023.

Table 1 illustrates that almost all data subject rights in the PDP Act could be exempted in virtually every aspect of personal data processing. Moreover, when closely observed, the exceptions provided were most likely only applicable to state and government institutions. The PDP Act categorised data controllers and processors into three categories, namely (a) Every Person (individual or a corporation), (b) Public Agency (state and government institutions), and (c) International Organisations. Based on the categorisation and comparison of the methods of exemption, only public agencies (public sector institutions) could use the reasons for the exemption of data subject rights.

The exclusion of Public Agencies from almost all obligations was principally against the spirit of the stipulations in the PDP Act (Alibeigi & Munir, 2020). Although the government mentioned on many occasions that the scope of the PDP Act covered both the public and private sectors (Hidayat, 2022), the exemptions above seemed to be only used by the public sector institutions. A typical example was the national defence and security, and law enforcement processes. The possibility of the private sector implementing the exemption was insignificant. Even when there might be exempted data subject rights, it was probably by request from law enforcers, which was also categorised as a public agency. The only exemption applicable to the private sector was for statistics and scientific research. This was different from the 2019 version of the PDP Bill, stating that data subject rights could be exempted for research "in the framework of government administration". In addition, it was similar yet different from the approach for research in the EU, where the derogation of data subject rights is possible for scientific research, even though the implementation might be challenging (Bell et al., 2019; Laurie & Stevens, 2016; Staunton et al., 2019).

The Indonesian PDP Act seemed to adopt a "partial" exemption approach. According to Alibeigi and Munir (2020), partial exemptions showed certain principles that did not apply to specific activities. An example could be observed in the Malaysian PDP Act, where some principles or provisions of the PDP Act did not apply to certain activities, such as journalistic, literary, and artistic activities, or to the detection of crime, investigation, taxation, statistics, or conducting research (See Section 45(2) of the Malaysia PDP Act 2010). Nevertheless, the Indonesian PDP Act also gave a kind of "total exemption" vibe in the sense that the exemptions were primarily applicable only to public agencies.[5] However, it

[5] According to Alibeigi and Munir (2020), total exemptions means that the PDP Act will not apply totally to (data processing) activities.

should be noted that the Malaysian and Singaporean PDP Acts had different positions, with the explicit exclusion of the public sector (Alibeigi & Munir, 2020; Islam et al., 2022). The Malaysian PDP Act 2010 excluded government institutions/public authorities as data controllers and processors (See Section 3(1) of the Malaysia PDP Act 2010), while the Singapore PDP Act 2012 exclusively applied to "organisations", which were essentially non-government institutions. Therefore, the Indonesian PDP Act seems to have unconsciously targeted non-government or private sector actors as its primary subject, but not completely.

An issue regarding the scope and limitations of these exemptions must be addressed. For instance, the Elucidation of Article 15 did not explain what "national defence and security purpose" meant and stated that it was "self-explanatory".[6] This raised a further question regarding the extent to which data processing activities were considered defence and security, and whether intelligence services and mass surveillance activities were included. Due to the confidential characteristic of the matter, individuals never knew to what extent their rights were protected or derogated and hence, must depend on a certain level of trust in public authorities (European Union Agency for Fundamental Rights, 2023; Hakkala & Koskinen, 2022). In addition, the secret nature also meant that it could be more challenging to ensure whether the exemptions were actually applied only to articles allowed to be exempted. This was also the case in the exemption based on public interest in government administration. The Elucidation of Article 15 only provided some examples of what constituted a public interest in government activities. This showed that the government could expand the interpretations of public interest in government activities.

This scenario could pose potential problems due to its failure to establish sufficient conditions for exceptions. The inadequacies often led to the infringement of data subject rights (Djafar & Syauqillah, 2022), excessive use of exceptions, and the unintended broadening of exception criteria. This expansion could occur when governmental activities were construed as being for government administration purposes and in the public interest, even when not expressly outlined in the PDP Act. However, the PDP Act actually provided some mitigations, such as by requiring data controllers to conduct data protection impact assessments (DPIA) (See Article 34) and appoint data protection officers (DPO) (See Article 53) when data processing was conducted, for instance, in public services, and for a large-scale data. This approach is similar to the EU General Data Protection Regulation (GDPR), which mandates DPIA and the designation of DPO for specific types of activities, including public sector data processing (See Article 35 and Article 37 of the GDPR). The implementation of the exemptions will largely be dependent on the meaningful enforcement of articles concerning the DPIA and the DPO so as to ensure that data subject rights remain protected and public agencies do not overuse the exemptions.

Provisions of Penalties and Remedies

The issue regarding various exemptions was related to the second issue concerning the provisions for penalties and remedies. The PDP Act accommodated two types of sanctions, namely criminal and administrative. Chapter XIV regulated criminal provisions for those violating the rights and obligations in the PDP Act. However, the subject used in various penalty provisions was "Every Person" (*Setiap Orang*). Article 1 number 7 of the PDP Act stated that "Every Person" is an individual or a corporation,

[6] Moreover, national defense and security were also included as an example for the scope of "public interest" as explained in the Elucidation of Article 3 letter c of the PDP Act about the principle of public interest. The full text is as follow: *"Principle of public interest" shall mean that in enforcing Personal Data Protection, it must take into account the interests of the public or society at large.* ***These public interests shall include*** *the interests of state administration and* ***national defense and security*** (emphasis added).

and "Corporation" showed a collection of people (and/or) assets in the form of a legal entity (*badan hukum*) or non-legal entity (*bukan berbadan hukum*). Although a "legal entity" could also refer to public institutions in a broader interpretation, the PDP Act used the term "Public Agency" to refer to public institutions. Therefore, the formulation showed that public institutions were excluded as the subject of sanctions.

Apart from the subject, the types of sanctions mentioned in criminal provisions were directed at private entities. For example, Article 70 paragraph (4) stated that in addition to (criminal) fines, a corporation could be imposed additional sentences, such as the "confiscation of profits and/or assets obtained or proceeds from crimes", "permanent prohibition of doing certain actions", or "shutdown of the entire or part of the corporation's place of business and/or activities". These types of sanctions obviously could not be imposed on public agencies. Considering the formulation, it could be argued that when public sector data controller obligations were violated, the individuals in charge might be criminally punished instead of the institution. Therefore, there was a high potential to criminalise "data protection officers" or individuals in charge of data processing in public institutions. Based on the formulation of criminal sanction provisions, it became more apparent that criminal sanctions were targeted at private entities, even though the PDP Act also applied to public sector institutions.

With respect to the administrative sanctions, the PDP Act did not refer to specific subjects but rather the types of violations. Article 57 paragraph (1) of the PDP Act referred to various articles related to data controller and processor obligations mentioned throughout the Act. However, there are two reasons why administrative sanctions are also prone to target private entities compared to public institutions. First, the PDP Act introduced various exemptions to derogate data controller and processor obligations. The majority of (if not all) exemptions mentioned in Table 1 above could only be implemented by public agencies, considering their nature. Second, the types of administrative sanctions mentioned in Article 57 paragraph (2), specifically related to the "temporary suspension of data processing activities" and the "erasure or removal of personal data", were most likely impossible to apply to government institutions, as it could interfere with the process of government administration and public service delivery that relied heavily on data processing (Blume, 2012; Rubinstein et al., 2014). The formulation of a paragraph concerning administrative fines also indicated that the article was formulated to mainly target the private sector, as the calculation of fines was based on annual income or annual revenue (See Article 57 paragraph (3) of the Indonesian PDP Act). Therefore, further questions also arose with regard to the question of how to determine the "annual income" or "annual revenue" of public institutions as the basis for imposing administrative fines.

Although the PDP Act applied to the public and private sectors, the formulation of criminal and administrative sanctions showed that public sector institutions were almost untouchable from both criminal and administrative sanctions. In addition, there was a slight potential for supervisory authority, which was mandated to impose administrative sanctions in the form of a written reprimand or administrative fines to public agencies, despite the issue of the basis for determining the number of administrative fines. Depending on the substance of the written reprimand or the amount (and mechanism) of imposing administrative fines, administrative sanctions imposed on public agencies potentially only became a formality and was therefore, not meaningful. A similar takeaway was also shared by Djafar from The Institute for Policy Research and Advocacy (ELSAM), stating that "*even with the same capacity as data controller, the implementation of sanctions will be more on corporations, but blunt on public agencies*" (Kompas, 2022; Septiani, 2022). Therefore, an independent supervisory authority was necessary to ensure that sanctions were proportional and appropriate.

Establishment of Supervisory Authority

This was where the third issue regarding the establishment of supervisory authority could be applied. The issue regarding the establishment of a supervisory authority was attracting scholars' focus, as the chapter on supervisory authority was missing from the 2019 PDP Bill. The majority of scholars agreed that the PDP Act must also regulate an independent supervisory authority to supervise the implementation of the PDP Act (Doly, 2021; Mahardika, 2021; Sabowo et al., 2022; Widiatedja & Mishra, 2022). The chapter concerning supervisory authority was later included in the final version of the PDP Bill enacted in 2022.

Regarding supervisory authority, Privacy International (2018) considered two personal data protection enforcement models, namely an independent supervisory authority and a ministry-based variant. Based on the adoption rate of the institutional model for personal data protection enforcement, 90% of countries with data protection laws opted for the first model (Privacy International, 2018). In addition, an independent authority was essential for oversight and enforcement. Therefore, the law that became the basis for establishing authority must provide the appropriate provisions concerning structure, mandate, and power to ensure the operation of this authority.

The PDP Act had a specific chapter regarding the establishment of a "data protection agency" (DPA). By the time of the writing of this article, the DPA had not yet been established. Moreover, the wording of the Act did not explicitly mention its independence. Article 58 of the PDP Act only stated that (emphasis added):

> *(1)* ***The government has a role in the realisation of the implementation of Personal Data Protection*** *in accordance with the provisions of this Act.*
> *(2)* ***The implementation of Personal Data Protection****, as referred to in paragraph (1) shall be* ***conducted by an agency.***
> *(3) The agency as referred to in paragraph (2) shall be* ***established by the President****.*
> *(4) The agency as referred to in paragraph (2) shall be* ***responsible to the President****.*
> *(5) Further provisions regarding the agency as referred to in paragraph (2) shall be regulated in a Presidential Regulation.*

This showed that the PDP Act delegated the establishment of an agency to the President. Therefore, it depended on the President to decide the institutional form of the DPA and whether to give independence to the agency. The PDP Act generally and thus, minimally regulated the DPA by only providing the mandate and power of the agency.

Looking back at the drafting process of the PDP Act, the provisions concerning the agency could be said to be a compromise between the government and the House of Representatives. On one side, the government wanted the DPA to be given to an executive agency. The House of Representatives wanted an independent DPA outside the executive, legislative, and judiciary branches. Consequently, the issue of the establishment of the agency stalled the discussion of the PDP Bill (Basyari et al., 2022).

Theoretically, several types of institutions were established based on the delegation from the Act, such as a non-structural state institution or an executive agency. Ideally, a non-structural state institution was a state institution outside the executive that was given independence in its legal basis (Asimow, 2002; Eddyono & Saptaningrum, 2007; Tauda, 2011). A non-structural state institution was usually led by collective collegial commissioners. The appointment of commissioners was conducted by more than

one branch of the state, mostly by the executive and legislative, and sometimes with the judiciary. However, several non-structural state institutions were responsible to the President and were stated explicitly in their Acts, such as the Competition Commission (KPPU), Child Protection Commission (KPAI), Broadcasting Commission (KPI), and Indonesian Medical Council (KKI). Although these institutions were responsible to the President, their legal basis also showed their independence.

The executive agency was an institution under the executive that carried out specific government duties, which were generally performed by more than one ministry. The head of an executive agency was appointed by the President and usually could be dismissed without the consent of another branch of the state. Therefore, one of the differences between a non-structural state institution and an executive agency was regarding its independence. Several studies have shown that there was no specific legal basis that differentiated non-structural institutions and executive agencies. This could be reflected in the existence of the various non-structural institutions that were independent by law, but were also responsible to the President (even though there is a discourse regarding the position of the President, whether as head of the government or head of the state).

Based on these results, creating an "independent" authority was actually possible despite what the PDP Act currently regulated. One of the prominent examples was the establishment of the Indonesian Prosecutor Commission. Although the mandate to establish the "commission" was stated in the Prosecutor Act (Law No. 16/2004 *jo.* Law No. 11/2021), the Act did not state anything about the form of the commission (as it could be a non-structural institution or an executive agency) and its independent status. The Presidential Regulation on Prosecutor Commission (Presidential Regulation No. 18/2011) reflected the choice to establish a non-structural institution and its independence. The Presidential Regulation gave an independent status to the commission. Therefore, the President chose an "independent" commission to supervise prosecutors despite the Prosecutor Act not saying anything about the commission's independence. This showed that even when the Act did not mention the commission's independence, it still could be given by another legal basis that it mandated.

In the context of an executive agency, there was a case where the legal basis for establishing the agency stated that it was "independent". This could be seen in Article 5 of the Zakat Management Act (Law No. 23/2011), stating that the *Badan Amil Zakat Nasional* (National Zakat Amil Zakat Agency or BAZNAS) was a "non-structural executive agency", was "independent" and responsible to the President through the Minister (of Religious Affairs). This was an interesting example of lawmakers creating an "independent" executive agency for the first time, which was generally below the executive.

Considering the current situation in Indonesia, amidst the various cases of personal data leakage, specifically, those held by government institutions, and their response to the leakage, establishing an independent DPA that could supervise public bodies was more favourable. When personal data protection was handled only by a government institution (as part of the executive), the potential for the breach cases to not being handled proportionally was higher, specifically when the case happened in the same and higher-level government or state institutions. This was reflected in data leak cases of the Social Health Insurance Administration Body (BPJS), eHAC, and the General Election Commission. In addition, creating an independent agency could increase public trust in the agency.

CONCLUSION

In conclusion, due to the series of data breaches that had occurred in recent years, specifically in various government institutions, along with the scattered regulations of personal data leading to sectoral and unstandardised protection, the enactment of a comprehensive PDP Act was expected to tackle these issues. The enactment of the PDP Act marked a significant milestone for Indonesia in the country's effort towards the comprehensive protection of individual personal data, considering Indonesia was among the countries that have produced the most extensive data globally. As discussed in the present article, various issues still need to be addressed to ensure the meaningful implementation of the PDP Act.

Based on the results of the investigation in this paper, other issues needed attention. These were matters which were closely related to the substance of the PDP Act. For instance, there was a tendency for sectoral institutions to use more "specialised" or "sectoral" Acts to avoid data protection obligations. It was mentioned in the closing chapter of the PDP Act that other Acts related to personal data protection which were still in force, provided there was no contradiction. In addition, these concerns had become a grey area, as they were dependent on the implementing institutions to interpret potential contradictions, specifically as the PDP Act has also provided various exemptions that could be broadly interpreted. Another example was a more technical aspect regarding the potential of no meaningful implementation of the PDP Act. This could be the case as the PDP Act has set a high standard for data processing for public services and vast amounts of personal data (albeit coupled with broadly interpreted exemptions), but has not been supported by the provision of qualified government officials to handle data protection issues. These examples have the potential to be further explored. Future studies could also delve into the more technological aspects of data protection, as well as the emerging issues of the use of AI in government administration and its impact on citizens' data protection by government institutions.

To achieve the meaningful implementation of the PDP Act in the public sector, the DPA could potentially become the vocal point. Therefore, the independence of the DPA must be explicitly mentioned in the Presidential Regulation, despite the form of institutional agency that the President had selected. In addition, it was essential to increase public trust in the state (specifically the government) and minimise the conflict of interest in implementing data protection. This showed that the government must prioritise the establishment of the DPA to ensure that the PDP Act could be meaningfully implemented. In parallel, the government also needed to start the harmonisation process of various Acts and their implementing regulations that previously regulated personal data, considering the many sectoral Acts that regulated personal data. This method was expected to help minimise the potential of government institutions to try to avoid data protection obligations using other Acts.

ACKNOWLEDGMENT

This article was supported by the 2021 Research Grant from the Faculty of Law, Universitas Gadjah Mada, Indonesia. The author reported no potential conflict of interest.

REFERENCES

Agostino, D., Arnaboldi, M., & Lema, M. D. (2020). New development: COVID-19 as an accelerator of digital transformation in public service delivery. *Public Money & Management*, *41*(1), 1-4. https://doi.org/10.1080/09540962.2020.1764206

Alibeigi, A., & Munir, A. B. (2020). Malaysian personal data protection act, a mysterious application. *University of Bologna Law Review*, *5*(2), 362–374.

Alsenoy, B. van, Kindt, E., & Dumortier, J. (2011). Privacy and data protection aspects of e-government identity management. In S. van der Hof & M. M. Groothuis (Eds.), *Innovating Government. Information Technology and Law Series Vol. 20*. (T.M.C). 251-282. Asser Press.

Asimow, M. R. (2002). *Administrative law*. Gilberts Law Summaries.

Basyari, I., Harbowo, N., & Kustiasih, R. (2022). Nasib pembahasan RUU perlindungan data pribadi kian suram. *Kompas.* https://www.kompas.id/baca/polhuk/2022/03/31/pembahasan-ruu-pdp-tak-dilanjutkan

BBC Indonesia. (2021, August 31). *Data eHAC milik 1,3 juta penggunanya dilaporkan bocor, 'keamanan data tidak prioritas*. BBC Indonesia. https://www.bbc.com/indonesia/indonesia-58393345

Bell, J., Aidinlis, S., Smith, H., Mourby, M., Gowans, H., Wallace, S. E., & Kaye, J. (2019). Balancing data subjects' rights and public interest research: Examining the interplay between UK law, EU human rights law and the GDPR. *European Data Protection Law Review*, *5*(1), 43–53. https://doi.org/10.21552/edpl/2019/1/8

Bhat, P. I. (2019). *Idea and Methods of Legal Research*. Oxford University Press.

Black, G., & Stevens, L. (2013). Enhancing data protection and data processing in the public sector: The critical role of proportionality and the public interest. *SCRIPTed*, *10*(1), 93–122. https://doi.org/10.2966/scrip.100113.93

Blume, P. (2004). Data protection in the private sector. *Scandinavian Studies in Law*, *47*, 297–318.

Blume, P. (2012). The inherent contradictions in data protection law. *International Data Privacy Law*, *2*(1), 26–34.

Blume, P. (2015). The public sector and the forthcoming EU data protection regulation. *European Data Protection Law Review*, *1*(1), 32–38. https://doi.org/10.21552/edpl/2015/1/7

Blume, P., & Svanberg, C. W. (2013). The proposed data protection regulation: The illusion of harmonisation, the private/public sector divide and the bureaucratic apparatus. *Cambridge Yearbook of European Legal Studies*, *15*, 27–46. https://doi.org/10.5235/152888713809813639

Boehme-Neßler, V. (2016). Privacy: A matter of democracy. Why democracy needs privacy and data protection. *International Data Privacy Law*, *6*(3), 222–229. https://doi.org/10.1093/idpl/ipw007

Brown, A., Fishenden, J., & Thompson, M. (2014). *Digitizing government: Understanding and implementing new digital business models*. Palgrave Macmillan.

Chik, W. B. (2013). The Singapore personal data protection act and an assessment of future trends in data privacy. *Computer Law and Security Review*, *29*(5), 554-575.

CNN Indonesia. (2020, May 21). *2,3 Juta data KPU diduga bocor, dijual di forum hacker*. CNN Indonesia. https://www.cnnindonesia.com/teknologi/20200521223601-185-505726/23-juta-data-kpu-diduga-bocor-dijual-di-forum-hacker

Djafar, W., & Syauqillah, M. (2022). Developing an equilibrium of protection of the right to privacy and national security in terrorism eradication in Indonesia. *Journal of Terrorism Studies*, *4*(2), 1–14.

Doly, D. (2021). Pembentukan lembaga pengawas pelindungan data pribadi dalam perspektif pembentukan lembaga negara baru. *Negara Hukum*, *12*(2), 223–244.

Eddyono, S. W., & Saptaningrum, I. D. (2007). Catatan umum atas keberadaan komisi negara di Indonesia. *Jurnal Legislasi Indonesia*, *4*(3).

European Union Agency for Fundamental Rights. (2023). *Surveillance by intelligence services: Fundamental rights safeguards and remedies in the European Union*. https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/02-28/FRASubmissiontothePEGACommittee_EN.pdf

Fahmi, A. B. (2020, July 6). Data pasien Covid-19 bocor dianggap tanggung jawab kemenkes. *Katadata*. https://katadata.co.id/yuliawati/digital/5f02f85af052d/data-pasien-covid-19-bocor-dianggap-tanggung-jawab-kemenkes

Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU*. Springer International Publishing.

Galuh, P. R. (2021, May 21). Data 279 juta penduduk yang bocor identik dengan milik BPJS, kominfo panggil direksi. *Kompas*. https://tekno.kompas.com/read/2021/05/21/14351007/data-279-juta-penduduk-yang-bocor-identik-dengan-milik-bpjs-kominfo-panggil

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*(3), 421–471.

Greenleaf, G. (2014). *Asian data privacy laws: Trade & human rights perspectives*. Oxford University Press.

Hakkala, A., & Koskinen, J. (2022). Personal data protection in the age of mass surveillance. *Journal of Computer Security*, *30*(2), 265–289. https://doi.org/10.3233/JCS-200033

Hert, P. De, & Gutwirth, S. (2006). Privacy, data protection and law enforcement. Opacity of the individual and transparency of the power. In E. Claes, S. Gutwirth, & A. Duff (Eds.), *Privacy and the Criminal Law* (pp. 61–104). Intersentia.

Holvast, J. (2008). History of privacy. In V. V. Matyas, S. Fischer-Hübner, D. Cvrcek, & P.Venda (Eds.), *The Future of Identity in the Information Society* (pp. 13–42). Springer-Verlag Berlin Heidelberg.

Islam, M. T., Sahula, M., & Karim, M. E. (2022). Understanding GDPR: Its legal implications and relevance to south asian privacy regimes. *UUM Journal of Legal Studies*, *13*(1), 45–76. https://doi.org/10.32890/uumjls2021.13.1.3

Keller, P. (2019). The reconstruction of privacy through law: A strategy of diminishing expectations. *International Data Privacy Law*, *9*(3), 132–152.

Kokott, J., & Sobotta, C. (2013). *The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR*. *3*(4), 222–228. https://doi.org/10.1093/idpl/ipt017

Kompas. (2022). Sanksi bagi lembaga publik dan swasta yang langgar UU PDP dinilai tak setara. *Kompas*. https://nasional.kompas.com/read/2022/09/22/05090091/sanksi-bagi-lembaga-publik-dan-swasta-yang-langgar-uu-pdp-dinilai-tak-setara

Kuziemski, M., & Misuraca, G. (2020). AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings. *Telecommunications Policy*, *44*(6).

Laurie, G., & Stevens, L. (2016). Developing a public interest mandate for the governance and use of administrative data in the United Kingdom. *Journal of Law and Society*, *43*(3), 360–392.

Lin, J., Carter, L., & Liu, D. (2021). Privacy concerns and digital government: Exploring citizen willingness to adopt the COVIDSafe app. *European Journal of Information Systems*, *30*(4), 389–402. https://doi.org/10.1080/0960085X.2021.1920857

Lynskey, O. (2014). Deconstructing data protection: The "added-value" of a right to data protection in the EU legal order. *International and Comparative Law Quarterly*, *63*(3), 569–597.

Mahardika, A. G. (2021). Desain ideal pembentukan otoritas independen perlindungan data pribadi dalam sistem ketatanegaraan Indonesia. *Jurnal Hukum UNISSULA*, *37*(2), 101–118.

Ministry of Communication and Informatics of the Republic of Indonesia. (2019, December 12).

Menunggu UU perlindungan data pribadi. *Indonesia.Go.Id*. https://www.indonesia.go.id/narasi/indonesia-dalam-angka/sosial/menunggu-uu-perlindungan-data-pribadi

Ministry of Communication and Informatics of the Republic of Indonesia. (2023, July 7). *Perkembangan penanganan gugaan kebocoran data paspor 34,9 juta warga Indonesia*. Ministry of communication and informatics of the republic of Indonesia. https://www.kominfo.go.id/content/detail/50065/siaran-pers-no-138hmkominfo072023-tentang-perkembangan-penanganan-dugaan-kebocoran-data-paspor-349-juta-warga-indonesia/0/siaran_pers

Muñoz, L. A., & Bolívar, M. P. R. (2018). Experiences of E-government development implementation in developing countries: Challenges and solutions. in L. A. Muñoz & M. P. R. Bolívar (Eds.), *International E-Government Development*. Palgrave Macmillan.

OECD. (2020). *OECD Digital Economy Outlook 2020*. OECD.

Otjacques, B., Hitzelberger, P., & Feltz, F. (2007). Interoperability of E-government information systems: Issues of identification and data sharing. *Journal of Management Information Systems*, *23*(4), 29–51. https://doi.org/10.2753/MIS0742-1222230403

Privacy International. (2018). *A guide for policy engagement on data protection: The keys to data protection*. Privacy International.

Rahman, F. (2021). Kerangka hukum perlindungan data pribadi dalam penerapan sistem pemerintahan berbasis elektronik di Indonesia. *Jurnal Legislasi Indonesia*, *18*(1), 81–102.

Rahman, F., & Wicaksono, D. A. (2021). Examining the reference of personal data interpretation in Indonesian constitution. *Jurnal Penelitian Hukum De Jure*, *21*(2), 187-200.

Regan, P. M. (1986). Privacy, government information, and technology. *Public Administration Review*, *46*(6), 629–634.

Rubinstein, I. S., Nojeim, G. T., & Lee, R. D. (2014). Systematic government access to personal data: A comparative analysis. *International Data Privacy Law*, *4*(2), 96–119.

Rumbold, J. M. M., & Pierscionek, B. K. (2018). What are data? A categorization of the data sensitivity spectrum. *Big Data Research*, *12*, 49–59.

Sabowo, H. K., Hartati, S., & Karyono, H. (2022). The urgency of personal data protection for the community: There is need for an independent commission. *International Journal of Educational Research & Social Sciences*, *3*(1), 413–424.

Septiani, L. (2022). *Ahli sebut pengesahan UU PDP terancam jadi macan kertas*. Katadata. https://katadata.co.id/syahrizalsidik/digital/6329c8ec9abcc/ahli-sebut-pengesahan-uu-pdp-terancam-jadi-macan-kertas

Sloot, B. van der. (2017). Legal fundamentalism: Is data protection really a fundamental right? In R. Leenes, R. Van Brakel, S. Gutwirth, & P. De Hert (Eds.), *Data protection and privacy: (In) Visibilities and Infrastructures* (pp. 3–32). Springer International Publishing.

Solove, D. J. (2008). *Understanding privacy*. Harvard University Press.

Staunton, C., Slokenberga, S., & Mascalzoni, D. (2019). The GDPR and the research exemption: Considerations on the necessary safeguards for research biobanks. *European Journal of Human Genetics*, *27*(8), 1159–1167. https://doi.org/10.1038/s41431-019-0386-5

Tauda, G. A. (2011). Kedudukan komisi negara independen dalam struktur ketatanegaraan republik Indonesia. *Pranata Hukum*, *6*(2).

Thompson, N., Mullins, A., & Chongsutakawewong, T. (2020). Does high e-government adoption assure stronger security? Results from a cross-country analysis of Australia and Thailand. *Government Information Quarterly*, *37*(1), 101408. https://doi.org/10.1016/j.giq.2019.101408

Thompson, N., Ravindran, R., & Nicosia, S. (2015). Government data does not mean data governance: Lessons learned from a public sector application audit. *Government Information Quarterly*, *32*(3), 316–322.

Van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3),

472–480.

Walters, R., Trakman, L., & Zeller, B. (2019). *Data protection law: A Comparative Analysis of Asia-Pacific and European Approaches*. Springer Singapore. https://doi.org/10.1007/978-981-13-8110-2

Widiatedja, I. G. N. P., & Mishra, N. (2022). Establishing an independent data protection authority in Indonesia: A future-forward perspective. *International Review of Law, Computers & Technology*, *37*(3), 1–22.

Wu, Y. (2014). Protecting personal data in E-government: A cross-country study. *Government Information Quarterly*, *31*(1), 150–159.

Xiao, C. (2019). Personal data rights in the era of big data. *Social Sciences in China*, *40*(3), 174–188.

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law and Security Review*, *35*(5), 1–11.