CONSTITUTIONALE
Volume 3 Issue 1, January-June 2022: PP: 21-42
Faculty of Law, Universitas Lampung, Bandar Lampung, Indonesia.
http://jurnal.fh.unila.ac.id/index.php/constitutionale
P-ISSN: 2723-2492 E-ISSN: 2745-9322

The Urgency of Independent Supervisory Authority Towards Indonesia's Personal Data Protection

Yulia Neta
Universitas Lampung, Indonesia
yulia.neta@fh.unila.ac.id

Agsel Awanisa
Universitas Lampung, Indonesia
agselawanisa17@gmail.com

Melisa
Universitas Lampung, Indonesia
melisanasir258@gmail.com

Submitted: Feb 15, 2022 ; Reviewed: Apr 27, 2022; Accepted: Jun 29, 2022

Article's Information

Keywords:
Independent Supervisory Authority; Personal Data Protection.

DOI:
https://doi.org/10.25041/constitutionale.v3i1.2535

Abstract

Abstract

In the Working Committee Meeting of the Draft Law on Personal Data Protection, there was a proposal to establish an Independent Supervisory Authority in the protection of personal data. With the existence of an independent supervisory authority, it is hoped that it will create impartial and optimal independence in its supervision and enforcement. The purpose of this study is to analyze the urgency of the Independent Supervisory Authority in the protection of personal data and the ideal concept of the Independent Supervisory Authority in the protection of personal data in Indonesia based on comparisons in other countries. This study uses a normative legal research method using a statutory approach, a conceptual approach, and a comparative approach. The results of this study indicate that the existence of an Independent Supervisory Authority in Indonesia in enforcing the protection of personal data is very important given the considerations of independence, adequacy, checks and balances, and socialization. Regarding the concept of establishing an Independent Supervisory

Authority, there are two choices that can be made in Indonesia, namely by establishing it specifically as a separate institution, such as Hong Kong and South Korea, or embedding and adding to the authority of existing institutions such as in Singapore and the United States. In Indonesia, by taking into account efficiency and effectiveness, this can be done by attaching an Independent Supervisory Authority with other related institutions such as the Information Commission with the obligation to change the existing institutional structure as an adjustment.

A. Introduction

The development of information and communication technology shows a significant increase. The development of information and communication technology can provide opportunities but also pose challenges at the same time.[1] Indonesia is a developing country in the Asia Pacific region, one of the most populous countries in Southeast Asia.[2] According to the general chairman of APJII, internet usage traffic in Indonesia until June 2020 increased by 20-25% from the previous data in 2018, which reached 171.17 million of the total population of Indonesia of 264.14 million people.[3] This makes Indonesia one of the most significant internet users in the world.[4]

The use of the internet (interconnection networking) which is a medium of information and electronic communication that provides a variety of activities in the form of services and products such as e-commerce (trade/business through electronic media), e-education (education), e-health (health), e-commerce -government (government), e-payment (finance), social media and others.[5] Almost all people use internet technology developed by private parties who are significantly at risk of violating the privacy rights of someone's data.[6] In addition, government agencies also need personal data to provide services and to plan health care and education delivery to citizens. However, more and more personal data and customer data are collected arbitrarily without the consent of the data subject.[7]

Personal data is collected passively through information technology without the data subject's consent. The protection of privacy rights and protection of personal data itself is an important aspect related to economic, social and cultural rights. According to Neethling et al., data protection, which refers to a person's legal protection is related to the processing of data about himself by another person or institution, namely the data controller.[8]

---

[1] Fanny Priscyllia,"*Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum*, JATISWARA, Vol. 34 No.3 November 2019, pg. 240.

[2] Budi Irawanto, "Making It Personal: The Campaign Battle on Social Media in Indonesia‟s 2019 Presidential Election‟ (11 April 2019), https://iseas.edu.sg, accessed on 31 December 2020.

[3]Deanne. Destriani., Firmansyah, Putri., & Fahrozi,Muhammad, Helmi., "Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)", *Procceding: Call for Paper 2 nd National Conference on Law Studies: Legal Development Towards A Digital Society Era, 2020, pg. 260.*

[4] Jeremias, Palito., Safira,A ,S., & Tiara,A,R.*,""Supremasi Hukum*", Volume 17 Nomor 1, Januari 2021. Pg. 24

[5] Dewi, S. (2016). "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia". *Demo2 Jurnal, (94), 22-30, pg. 23.*

[6] Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R. (2018). "Legal Protection for Urban Online-Transportation-User's Personal Data Disclosure in the Age of Digital Technology". *Padjadjaran Journal of Law, 5(3), 485-505, pg. 487-488*

[7] Jeremias Palito, *Op.Cit.*, pg. 24

[8] *Ibid.*

Concerning the protection of personal data, the Indonesian government has ratified the Covenant on Civil and Political Rights (ICCR), ratified through Law No. 12 of 2005 which affirms that the Indonesian government is obliged to protect the privacy and personal data of its citizens.[9] The right to privacy including the protection of personal data is recognized as a constitutional right of citizens as stated in CHAPTER XA Article 28A-28J of the 1945 Constitution of the Republic of Indonesia. Provisions regarding the guarantee of personal data protection can be found in Article 28 G paragraph 1 of the Law. The 1945 Constitution of the Republic of Indonesia states that "Everyone has the right to the protection of personal data, family, honor, dignity, and property under him, and has the right to a sense of security from threats to do or not do something which is a human right."[10]

Even though it has been stipulated in the constitution, Indonesia does not yet have any special rules in personal data protection regulation. Personal data protection is regulated at various levels of legislation in various sectors, namely the Telecommunications Law, KIP Law, ITE Law, Population Administration Law, Health Law, Banking Law, Human Rights Law, and Consumer Protection Law.[11] So this makes it difficult to use the legal principle of lex specialist when there is a general case and can be subject to various laws and regulations. Therefore, in Indonesia, there is still a need for rules governing the protection of personal data as a whole so that previously it was spread in various sectors. Become a comprehensive and concurrent arrangement.

The urgency of the protection of personal data is increasing because personal data can be misused and injure the rights of the owner of the personal data. There are even people who do not know at all about their privacy rights. The lack of public awareness of the importance of protecting personal data and fulfilling the right to privacy is an implication of the absence of a law that requires the protection of personal data.[12] Based on 2021 data, personal data leaks reached 279 million Indonesian citizens.[13] For this reason, the Personal Data Protection Bill (PDP) is currently being ratified in the queue at the 2021 Priority National Legislation Program (Prolegnas) for the ratification process, promising legal certainty regarding the protection of privacy and personal data in Indonesia.[14]

This also considers the number of personal data protection violations based on complaints. Based on the classification of PSEs who violated personal data protection, among others: E-commerce 39.3%, public agencies 14.3%, fintech operators 10.7%, consulting services 7.1%, insurance 7.1%, telecommunications 7.1%, social media 3.6%, others 10.8%. Based on this data, E-Commerce is the most significant percentage contributor to personal data breaches during 2019-May 2021. In contrast, the second largest contributor is public agencies.[15] For this reason, it is necessary to establish an independent supervisory authority in terms of personal data protection so that in its implementation, it can reach the supervision of various parties, both private institutions and public or government agencies.

---

[9] Upik Mutiara, Romi Maulana,"Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi", Indonesian Journal of Law and Policy Studies | *Volume 1 No. 1 Mei 2020, pg. 44.*

[10]Pasal 28G Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

[11] Wahyudi Djafar, "Makalah disampaikan sebagai materi dalam kuliah umum" *"Tantangan Hukum dalam Era Analisis Big Data"*, Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada, Yogyakarta, 26 Agustus 2019.pg. 5.

[12] Muhammad Saiful Rizal,"Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia*", Jurnal Cakrawala Hukum, Volume 10 No. 2 Desember 2019, pg. 221.*

[13]https://www.dw.com/id/data-279-wni-bocor-desakan-uu-perlindungan-data-mencuat/a-57638257.

[14]Jeremias Palito, *Op.Cit.*,Pg. 28.

[15]https://kominfo.go.id/content/detail/15455/mengulas-tiga-klasifikasi-data-dalam-revisi-pp-pste/0/sorotan_media, diakses pada tanggal 17 October 2021.

For this reason, it is necessary to establish an independent supervisory authority in terms of personal data protection so that it can supervise various matters in its implementation. During the Working Committee Meeting (Panja) of the Draft Law (RUU) on Personal Data Protection (PDP) between the Commission and the government to discuss the Problem Inventory List (DIM), one of which is related to the proposal of several factions regarding the establishment of a personal data protection supervisory authority who will be the supervisor in the implementation of the law. The authority will later function for enforcement investigations up to the imposition of sanctions. The government in the Personal Data Protection Bill DIM regulates the supervisory authority for personal data protection as the Data Protection Authority (DPA) or the Data Protection Authority, both private institutions and public or government agencies.[16] The critical role of this independent authority is not only in implementing privacy and data protection policies but also in terms of awareness raising, consulting and network development. Data protection authorities not only function as ombudsmen, auditors, consultants, educators, policy advisors and negotiators, but must also be able to enforce the law when private or public actors violate data protection laws.[17]

The discussion regarding the independent supervisory authority in protecting personal data is very important to put forward, considering that Indonesia currently does not have a particular institution that oversees the protection of personal data as a whole. Meanwhile, in many countries, independent institutions have already as supervisors for personal data protection, including France, South Korea, Hong Kong, Singapore, Germany, and the United States of America.

The Personal Data Protection Bill discussion is included in the 2021 Priority National Legislation Program. Earlier in the working committee meeting of the Personal Data Protection Bill, the government had asked to draw up a regulation regulating the independent Personal Data Protection supervisory authority. The substantive analysis is very much needed in the discussion of the Personal Data Protection Bill regarding the ideal format of an independent authority, namely an authority that is not under the government with the task of socializing, supervising, handling administrative disputes and mediation, as well as providing recommendations regarding the protection of personal data.[18]

Based on the description above, the purpose of this paper is to examine and analyze the urgency of an independent supervisory authority in the protection of personal data in Indonesia and the ideal concept of an independent supervisory authority in the protection of personal data in Indonesia based on comparisons in other countries. In conducting research, the author uses normative research methods.[19] It is carried out using a statutory approach, a concept approach, and a comparative approach.[20]

The author examines the urgency of an independent supervisory authority in protecting personal data related to the mechanism of the supervisory authority. This research is expected to be able to analyze the substantive in the protection of personal data. The novelty of this research is expected to be able to contribute in terms of protecting personal data which is a personal right with the existence of a supervisory authority.

---

[16] Ahmad Budiman," Otoritas Pengawas Perlindungan Data Pribadi", *info singkat, Vol. XIII, No.5/I/Puslit/Februari/2021, pg. 26.*

[17] Ahmad Budiman, *Op.Cit.*,Pg. 27.

[18]Ibid.

[19]I Gede A.B.Wiranata, *Metode Penelitian Dan Penulisan Ilmiah Bidang Hukum*, (Bandar Lampung: Zam Zam Tower, 2017), 60.

[20]Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana Prenada Media Group,2012), 93.

B. Discussion

1. The Urgency of Having An Independent Supervisory Authority in The Protection of Personal Data in Indonesia

Personal data relates to a person's characteristics, name, age, gender, education, occupation, address, and position in the family.[21] Warren and Brandeis stated, "Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded legal recognition." This means that privacy is a right for everyone to enjoy life and demands that their privacy is protected.[22] Van Der Sloot also stated that the term personal data includes not only sensitive or private data but also public and non-sensitive data.[23] The right to privacy of personal data must be carried out and the protection of personal data as a right to privacy is a constitutional right of Indonesian citizens as stated in the constitution, namely the 1945 Constitution of the Republic of Indonesia.[24]

Indonesia has ratified the ICCPR through Law Number 12 of 2005 concerning the International Covenant on Civil and Political Rights Ratification. Thus it can be concluded that the Government of Indonesia firmly supports the efforts of the international community to protect the right to privacy as outlined in these international instruments. The ratification is the right step because Indonesia has recognized the right to privacy in its constitution. This has been explicitly stated in the Indonesian Constitution, namely the 1945 Constitution (UUD 1945).[25] It is stated in Article 28 G paragraph (1): "Everyone has the right to personal protection, family, honor, dignity, and property under his control, and has the right to a sense of security and protection from the threat of fear to do or not do something wrong. is a human right". Then it is also stated in Article 28H paragraph (4) "Everyone has the right to have private property rights and such property rights may not be taken over arbitrarily by anyone."

In Indonesia, there are several regulations governing the protection of personal data, namely:[26]

a. Article 28G and Article 28J of the 1945 Constitution of the Republic of Indonesia.
b. Constitutional Court Decision Number 006/PUU-I/2003
c. Law Number 17 of 2007 concerning Long-Term National Plan Development 2005-2025
d. Law Number 39 of 1999 concerning Human Rights
e. Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration
f. Law Number 36 of 2009 concerning Health
g. Law Number 11 of 2008 concerning Information and Electronic Transaction
h. Law Number 14 of 2008 concerning Public Information Disclosure
i. Law Number 10 of 1998 concerning Banking
j. Law Number 8 of 1999 concerning Consumer Protection
k. Government Regulation Number 82 of 2012 concerning the Implementation of Electronic Systems and Transactions

[21]Mahira, DF, Emilda YLisa NA, "Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept", *Legislatif, Vol.3 No.2, 2020, pg. 288.*

[22]Rosadi, SD, 2015, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* Refika Aditama: Jakarta, pg. 23.

[23]Faiz Rahman,"Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia*", Jurnal Legislasi Indonesia Vol 18 No. 1 - Maret 2021, pg. 85.*

[24]Sekaring Ayumeida Kusnadi1 dan Andy Usmina Wijaya,"Perlindungan Hukum Data Pribadi Sebagai Hak Privasi", *Aiwaath Jurnal Ilmu HukumVolume2No. 1April202, pg. 11.*

[25]Rudi Natamiharja and Stefany,"Perlindungan Hukum Atas Data Pribadi di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi Pt.Telekomunikasi Selular)."*Prodigy Jurnal Perundang undangan, Mindoria,2019.pg. 10.*

[26]Padma Widyantari dan Adi Sulistiyono,"Pelaksanaan Harmonisasi Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP*)",Jurnal Privat Law Vol. VIII No. 1 Januari-Juni 2020, pg. 119.*

l. Regulation of the Minister of Communication and Information Number 20 of 2016 concerning the Protection of Personal Data in Electronic Systems.

From some of these regulations there is disharmony. This makes it challenging to use the legal principle of lex specialist when a case is general and can be subject to various laws and regulations. Therefore, it is necessary to have a legal unification that regulates personal data protection so that what was previously spread in various sectors becomes a comprehensive and concurrent arrangement.[27] Apart from the fact that there are so many rules regarding the protection of personal data in various laws and regulations, another quite crucial factor is the number of cases of misuse of personal data and the unclear sanctions for perpetrators who steal or sell personal data. These factors are the impetus for the Government and the House of Representatives to take the initiative to formulate the Personal Data Protection Bill (RUU PDP).[28]

The Personal Data Protection Bill has not yet been ratified and promulgated. However, in the Working Committee Meeting (Panja) of the Draft Law (RUU) on Personal Data Protection (PDP) between Commission I and the government discussed the Problem Inventory List (DIM), one of which was related to the proposal of several factions regarding the establishment of a personal data protection supervisory authority. Who will be the supervisor in the implementation of the law.[29]

After a long and intense reform, the European Union (EU) adopted a new Regulation (EU) on 27 April 2016 on the protection of individuals with respect to the processing of general personal data called the data protection regulation (GDPR). GDPR establishes a new system using a risk-based approach. This new approach is implemented through an integrated data protection system close to the data controller and processor and can adapt to various processing contexts.[30] "Personal data" is one of the critical notions of data protection law determining the material scope of the DPD and the GDPR. Only when personal data is processed do the data protection principles, rights and obligations apply (Article 3(1) DPD and Article 2(1) GDPR).[31]

The primary rationale of any regulation on personal data aims to avoid the realization of privacy risks, namely the occurrence of so-called personal data breaches which are defined as security breaches that lead to the destruction, loss, alteration, unauthorized disclosure of, or access to, personal data that is sent, stored, or otherwise processed. Because personal data breaches can, if not handled in an appropriate and timely manner, result in physical, material or non-material harm to natural persons, such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, unauthorized reversal of pseudonyms, damage to reputation, loss of confidentiality of personal data protected by professional confidentiality or other significant economic or social loss.[32]

Three different possible legal grounds for the right to an explanation of automated decision-making can be found in the GDPR. The right to explanation may be obtained from safeguards against automated decision-making as required. These bases are referred to as rights to explanations derived from (i) security, (ii) notification duties, and (iii) access rights,

[27]Nadiah Tsamara,"Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara", *Jurnal Suara Hukum, Vol. 3, No. 1, Maret 2021, pg. 30.*

[28] Glenn Wijaya,"*Pelindungan Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum*", Law Review Volume XIX, Nomor 3 – Maret 2020, pg. 329.

[29]Ahmad Budiman, *Op. Cit*., pg. 26.

[30]Gauthier Chassang*,"The impact of the EU general data protection regulation on scientific research"*, Ecancermedicalscience. Januari 2017, 11: 709, p.79.

[31] Nadezhda Purtova,"*The law of everything. Broad concept of personal data and future of EU data protection law",* Law, Innovation And Technology, 2018 Vol. 10, No. 1, p. 43.

[32] Gauthier Chassang, *Op.Cit.* p.79.

respectively. We will assess each one in turn. Overall, the claim that the GDPR grants a right to an ex-post explanation of certain (minimum) decisions that appears to apply to any instance of automated decision-making is based on a combination of protection and notification duties.[33]

The protection of personal data there are several principles of personal data protection as a fundamental right, among others:[34]

a. Privacy
   Privacy can be defined in various ways, such as the right to the confidentiality of communications, the right to be left alone, the right to self-regulate or the right to protect personal data. Privacy also illustrates the importance of the calm aspect between the individual and society. Meanwhile, privacy is concept-based based on people's perceptions of interests and benefits.[35]

b. Autonomy
   Everyone should have control over their data. The principle of autonomy and the related focus on consent is also clearly linked to the concept of dignity. Autonomy is the right of self-government. In fact, what is happening now is a violation of democratic principles and the rule of law: data collection, exchange, and processing have the potential to undermine central values such as individual autonomy and information self-determination as well as the fundamental rights of privacy, data protection and non-discrimination.

c. Transparency
   Transparency is openness, clarity, and not trying to hide damaging information. It is used in financial disclosures, organizational policies and practices, law-making, and other activities in which organizations interact with the public. GDPR tries to define 'consent' as an indication statement or by explicit affirmative action indicating consent to personal processing data. It is for this reason that De Hert and Gutwirth have argued that while the right to privacy could be defined as a tool of opacity that sets limits for the normative exercise of power, the right to data protection is a tool of transparency, which channels the exercise of that normatively accepted power.[36]

d. Non-discrimination
   The rights to personal data protection and non-discrimination interact differently and need to be increased in effectiveness. Regarding data processing technology, there are two complementary aspects of data protection and non-discrimination rights: the type of data covered by the protection and the type of control provided.

For this reason, in protecting personal rights which are private rights based on these principles, an independent supervisory authority is needed the protection of personal data in Indonesia. With the existence of an Independent Supervisory Authority in data protection, it is not only expected to function as a supervisory agency in implementing personal data protection in the community. Still, it is also expected to be able to change behavior for all parties in protecting personal data. This institution needs to have the power to supervise the protection of

[33] Sandra Wachter, Brent Mittelstadt and Luciano Floridi,"*Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation",* International Data Privacy Law, 2017, Vol. 7, No. 2, p. 14.

[34] Russel Butarbutar,"Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia", Atlantis Press SARL, Advances in Economics, Business and Management Research, *volume 130 3rd International Conference on Law and Governance (ICLAVE*), 2019, *p.* 155.

[35] Y. Mc Dermott, *"*Conceptualising the right to data protection in an era of Big Data,"Big Data Soc., *vol. 4, no. 1, p. 2053951716686994., 2017.*

[36] Yvonne McDermott*,"Conceptualising the right to data protection in an era of Big Data",* Big Data & Society, Sage Journal, January-June 2017, p. 3.

personal data, not only overseeing the private sector but also the public sector, namely executive, legislative, and judicial bodies or institutions.[37]

An independent data protection authority is a public institution whose function is to ensure the protection of personal data and the compliance of controllers and processors of personal data, both individuals or private entities and public institutions, to the laws and regulations related to data protection. This institution is one of the keys in personal data protection efforts, which is to function as the spearhead of privacy and data protection regulators. The agency's key role is overseeing the implementation of privacy and data protection policies, awareness raising, consulting, and network development. It takes institutional independence, personal human resources, and functions and authorities from the personal and political domains.[38] In summary, this independent authority must supervise, monitor and enforce the application of personal data protection laws. In carrying out this mandate, this institution needs to be equipped with an investigation function, namely conducting investigations and following up on public complaints. It can issue binding orders and impose penalties when they find that an institution or other body has violated the law. This also includes the ability to request information from data controllers or processors, perform audits, and gain access to all information needed for investigation purposes, including physical access to buildings or equipment used for processing if necessary.[39]

Regarding the effectiveness and success of enforcing the legal system, Lawrence M. Friedman has to touch on three legal components, which include: (a) legal structure, (b) legal substance, (c) legal culture).[40] The definition of structure is the court system. Especially in establishing an information technology legal system, it is necessary to prepare the extent to which courts in Indonesia can resolve cases of privacy violations. The existence of an independent authority will create an impartial and optimal law enforcement structure in its supervision and enforcement. The second element is the substance related to the contents of the legislation, which includes:[41]

a. Legal actions to be regulated.
b. The foundations to be applied are philosophical, juridical, and sociological.
c. The principles will be the basis of national and international legislation that does not injure the sovereignty of the State and Pancasila.

At this time, judges in resolving cases of violation of privacy are still based on beliefs and interpretations, so it cannot be said that there is a unification of thought that ultimately requires a regulation that can accommodate and keep up with changing times, especially in this case related to information technology law. Related to legal culture, a legal system that can be appropriately created is also determined by the extent to which people's behavior in perceiving the law through the mechanisms of legal traditions used to regulate the life of a society. Indonesian legal culture has the characteristic that the legislature forms laws at the suggestion of the relevant departments through input from the community.[42]

---

[37] *Ibid.*
[38]Ahmad Budiman, *Op.Cit.,* Pg. 27.
[39]*Ibid., pg 28.*
[40]Lawrence M.Friedman, (1977), Law and Society, an introduction, Prentice H.l, New Jersey, h. 35.
[41]Lawrence M. Friedman, 2009, *System Hukum Dalam Perspektif Ilmu Sosial*, The Legal System: A Sosial Science Perspektive, Nusa Media, Bandung, pg 16. Diterjemahkan dalam buku Lawrence M. Friedman, 1969, *The Legal System: A Sosial Science Perspektive, Russel Soge Foundation, New York*. pg. 53.
[42]Sinta Dewi, (2016), Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia, *Jurnal Yustisia, Vol. 15, No.1 , h. 29.*

For this reason, concerning the urgency of the ratification of the Personal Data Protection Bill, at least several things can be used as a basis for consideration, namely:

a. Independency

The establishment of this independent authority is essential, considering that this institution supervises controllers and processors of data from the private sector and oversees data controllers and processors of public bodies (government). With the existence of an independent supervisory authority, it will realize independence in supervision and enforcement. Regarding establishing an independent authority, what should be paid attention to is how independent the authority is. Based on Article 52 of the EU GDPR, a personal data protection authority must at least be formulated into five independence prerequisites, namely:[43]

1) In institutional independence, each supervisory authority must act with complete independence in carrying out its duties and exercising its powers following the law.
2) The independence of the commissioner, a member of the supervisory authority, in carrying out his duties and authorities following the law, free from external influences, either directly or indirectly, and will not carry out instructions from anyone. In addition, members of an independent supervisory authority must be able to refrain from acts that are inconsistent with their duties. During their tenure, they also do not engage in work that is not suitable for them, whether profitable or not.
3) The independence of the organization, the state must ensure that each supervisory authority is equipped with the human, technical and financial resources, buildings and infrastructure necessary for the effective implementation of its duties and authorities, including those to be carried out in the context of mutual assistance, international cooperation, etc.
4) In the independence of human resources, the state must ensure that each supervisory authority chooses its staff subject to the law or members of the supervisory authority concerned.
5) Financial control must not affect independence. Therefore the state must ensure that every supervisory authority is subject to financial control.

For this reason, in establishing an independent supervisory authority, it is necessary to consider some of these things so that they are genuinely independent authorities and are not under the auspices of the government or the executive. In principle, the data protection authority is expected to function as a supervisory agency and must be able to enforce behavior changes that do not violate data protection laws. The task of this authority is to supervise private entities and public authorities, namely executive, legislative, and judicial bodies or institutions, regarding the protection of personal data. The existence of an independent authority will create an impartial and optimal law enforcement structure in its supervision and enforcement.

b. Adequacy

The existence of an independent supervisory authority is one element in determining the level of legal equality in the protection of personal data that applies in the European Union with other countries. Based on the principle of special arrangements in the protection of personal data, a country can be adjusted for equality, in particular by looking at the regulatory model in the European Union regarding *On The Protection Of Natural Persons Concerning The Processing Of Personal Data And On The Free Movement Of Such Data, And Repealing Directive (EU GDPR)* which includes the scope: EU GDPR regulations on the protection of personal data should at least contain:

[43] Wahyudi Djafar M. Jodi Santoo, *Op. Cit*., Pg. 7.

(1) Lawfulness, fairness, and transparency.
(2) Purpose limitation.
(3) Data minimization.
(4) Accuracy.
(5) Storage limitation.
(6) Integrity and confidence.
(7) Accountability.

In Indonesia, the protection of personal data has been regulated in several regulations such as Law Number 23 of 2006 concerning Population Administration Juncto Law Number 24 of 2013 concerning Amendments to Law Number 23 of 2006 concerning Population Administration, Government Regulation of the Republic of Indonesia Number 71 2019 concerning the Implementation of Electronic Systems and Transactions, Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Protection of Personal Data in Electronic Systems and Regulation of the Minister of Communication and Information Technology Number 4 of 2016 concerning Information Security Management Systems are evidence of the embodiment of legal protection for personal data from the State Indonesia to data owners.[44] However, the spread of personal data protection provisions in various regulations causes disharmony in the application of the law, so legal unification and system improvement are needed, one of which is by formulating the existence of an independent supervisory authority.

Personal Data is also explicitly regulated in the EU GDPR, especially in Article 9 which concerns the principles of personal data protection as follows:[45]

1) Personal data must be processed in a legal, fair and transparent manner, such as:
   a. Obtained following the intended use, clear, specific except for public, scientific and research purposes.
   b. Relevant and limited according to its intended
   c. Guaranteed accuracy.
   d. Limited storage
   e. Guaranteed security, integrity and confidentiality
2) Rights of the owner of Personal Data: can see the regulatory model of the EU GDPR in particular Chapter III, namely the right of data subjects to information transparency in terms of processing their data, the right to access information to collect personal data (contracts, controllers), the right to delete and correct his data, the right to object to the processing of his personal data, the right to limit the processing of his personal data.
3) Controllers and processors: can see the regulatory model of the EU GDPR, in particular Chapter IV regarding the responsibility of the controller, who is the controller, the processor, the responsibility of the processor in the security of personal data, the form and mechanism of personal processing data.
4) Code of Ethics and certification: can see the EU GDPR regulatory model, especially Article 40 regarding the code of ethics for controllers and processors of personal data established by the Government, in addition to the Certification of controllers and processors of personal data by the government or certain government agencies.

[44] Amboro,F.Y.P,. Pusvita,P.2021. Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia)https://journal.uib.ac.id/index.php/combine.Volume 1 No 1 (2021)

[45]Ketut Sukawati Lanang Putra Perbawa,"*Konsep Dan Prinsip Pengaturan Perlindungan Data Pribadi Di Indonesia", Prosiding Seminar Nasional L FH UNMAS Denpasar "Urgensi dan Implikasi RUU Perlindungan Keamanan Kerahasiaan Data Diri Berbasis Digitalisasi",* pg. 42.

5) Transfer of personal data to other countries or international organizations: see the EU GDPR regulatory model in particular Chapter V that countries that are receiving personal data transfers must have the same regulatory standards for the protection of personal data. Independent supervisory authority: can look at the EU GDPR regulatory model, especially Chapter VI, where the authority is responsible for overseeing the personal data protection arrangements according to established regulations independent of external influences which can also serve as a forum for dispute resolution.
6) Compensation, liability and sanctions can see in the regulatory model of the EU GDPR in particular Chapter VIII that for example, the owner of personal data can ask for compensation from the controller and/or processor if his data is misused and processed not following the purpose or there is a violation.

Based on the provisions of the EU GDPR, there is a requirement for an independent supervisory authority in the protection of personal data. For this reason, so that Indonesia can become a country that is recognized for its legal equality for personal data protection or adequate as is the case in the European Union with other countries, Indonesia must be able to establish an independent supervisory authority. In this way, the legal equality of the protection of personal data will be recognized by the United Nations. If equality is recognized, it will provide many advantages for the Indonesian state. Among them can establish good cooperation with other countries in the context of law enforcement of personal data protection. With the existence of a digital or industrial economy, what is unavoidable is the existence of cross-border data flows, where which require adequate recognition for a country so that they can cooperate reasonably with each other. Countries considered to have met the adequacy include Andora, Argentina, Canada, Faroe Island, Guernsey, Isle of Man, Switzerland, Uruguay, Israel, Japan, Jersey, New Zealand, United States of America.

c. Check and Balance

The most significant benefit of having an independent supervisory authority is the ability to share and minimize differences of opinion between the functions of protecting personal data and disclosure of information. Having an independent supervisory authority can also reduce the potential and possibility of inter-institutional conflict, because in practice, many requests for information that fall under the jurisdiction of information disclosure laws will relate to personal information. In other words, the disclosure of public information often collides with the provision of personal data protection. For this reason, it is necessary to pay special attention to this problem. For this reason, the unification of bodies or institutions with these two functions will allow for a better balance. It will also make it easier for the general public to have contact with public bodies so that they can make better use of their rights. In other words, the existence of this independent supervisory authority acts as a mediator between the data controller and the data subject.[46]

Besides that, it is necessary to distinguish between data controllers and data processors. Such as the concept emphasized by the GDPR that the role of data controllers is as the party responsible for data and imposes controls and even stricter obligations on processors. This happens because some companies try to evade privacy responsibilities by declaring themselves "processors" while making decisions as controllers make. In Principle, the primary responsibility lies with the controller to provide the Data Protection Authority with detailed information to demonstrate that they have acted prudently and lawfully. The records created

[46] Ahmad Budiman, *Op.Cit*., 29.

should contain information such as which personal data were processed, why, who had access to them, how long they were stored and what security measures were in place.[47]

d. Socialization

There are many cases of personal data protection violations based on complaints, based on the classification of PSEs who violate personal data protection, including: E-commerce 39.3%, public agencies 14.3%, fintech operators 10.7%, consulting services 7.1%, insurance 7.1%, telecommunications 7.1%, social media 3.6%, others 10.8%. Based on this data, E-Commerce is the most significant percentage contributor to personal data breaches during 2019-May 2021.

The increase in the need for information and communication technology causes various criminal acts to appear which can result in material and immaterial losses for a person. The increasing number of activities of internet users causes cases regarding the protection of personal data to become severe and at risk of leakage of someone's personal data. The personal data burglary that occurred in 2011 was 25 million Telkomsel customers, and then the same thing happened again in September 2019 yesterday there was a leak of passenger data by Lion Air and Batik Air airlines which reached tens of millions of data. Leaked passenger data, including Identity Card (KTP) and passenger passport numbers accessed in Amazon Web Services (AWS) cloud computing accessed via the web stored in backup files in May 2019 for Malindo Air and Thai Lion airlines Water. Leaked data is very vulnerable to misuse, leading to several criminal acts such as identity theft or fraud, especially considering the current modern economic development towards a digital economy based on a creative economy. For business people, personal data is included as essential information. Norton Report 2013 data notes that the level of potential and risk for cybercrime in Indonesia is entering an emergency status and continues to increase, which is compiled from the official website of the Indonesia Security Incident Response Team on Internet Infrastructure.[48]

Lack of public awareness of the importance of protecting personal data and fulfilling their right to privacy. This happens because people do not know at all about their privacy rights. Thus, this socialization aspect can be carried out as a structuring of personal data protection activities, overseeing their implementation, handling administrative disputes and conducting non-litigation mediation and adjudication related to PDP issues, providing recommendations to data controllers or data processors and coordinating and delegating criminal-related issues to the police.[49] In addition, with its independent authority, this institution can focus on socializing, such as explaining the interpretation of regulations to increase the public's understanding so that the public can prevent misuse of personal data. We know that the ministry already has this socialization task, but the ministry has a lot of responsibility for various laws and regulations. So we need a special authority that can carry out the task of socializing this personal data protection.

The need for an Independent Authority in the protection of personal data in Indonesia in the Personal Data Protection Bill is presented to provide the tasks, functions, and powers of the data protection authority. From the start, the government has always reasoned about the prohibition of forming new institutions for efficiency reasons. However, given the scope of the Personal Data Protection Law, which is also binding on the private sector and public-government bodies, the existence of an independent supervisory authority is very much needed. Moreover, considering the large number of personal data processed by government data controllers and public bodies, it isn't easy to guarantee independence in supervision, if this

[47] Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius*,"The European Union general data protection regulation: what it is and what it means",* Information & Communications Technology Law 2019, Vol. 28, No. 1,p. 85.
[48]Fanny Priscyllia, *Op.Cit.*,pg. 241
[49]Ahmad Budiman, *Op.Cit*.,pg 30.

function is carried out by fellow government institutions. To implement this law's extraterritorial jurisdiction principle, the need to ensure the legal adequacy of Indonesian personal data protection with other countries. In addition, the principle of single authority (independent) will also provide convenience for data controllers in ensuring compliance, as well as the rights of data subjects in making claims for their rights. And also, the existence of an independent authority can focus more on providing socialization of the regulations and interpreting the meaning of the applicable regulations.

2. The Ideal Concept of An Independent Supervisory Authority in The Protection of Personal Data in Indonesia is Based on Comparisons in Other Countries

The protection of privacy for personal data in the European Union has been regulated as a fundamental right of citizens in The European Union Charter of Fundamental Rights. The European Union has legislation regarding personal data, namely The General Data Protection Regulation (GDPR). The regulation is a form of fulfillment of the fundamental rights of the European Union in the current digital era. The European Union has even established an institution, namely The Police Directive as an institution that functions as supervision and protection for citizens in terms of personal data processing and provides sanctions for any violations of the use of personal data committed against the owner of personal data. GDPR applies control rules to every process of personal data information used as a standard data protection rule in European Union countries.[50] One of the principles of personal data protection as stipulated in The General Data Protection Regulation (GDPR), is the existence of an independent supervisory authority. Before analyzing and looking at the implementation of independent supervisory authorities in other countries, it is necessary first to understand the models of data protection authorities in various countries, namely:[51]

a. Multi Authority Model

Some countries that apply this model in monitoring personal data protection are the United States and Canada. Through several laws, multi-agency policies are influenced by legislative policies or the establishment of sectoral data protection rules. An example of a country that applies sectoral data protection laws is the United States. In fact, this country has hundreds of laws and regulations relating to privacy and personal data protection, both at the federal and state levels. Twenty-five state laws relating to data privacy and privacy, including the California Consumer Privacy Act of 2018 (CCPA).

The many privacy and data protection regulations in the United States have implications for the many institutions that function as supervisors to implement these various laws. However, especially for the private sector, almost entirely run by the Federal Trade Commission (FTC), which is an independent regulatory agency that has been established since 1914. This institution was formed to monitor companies and protect consumers from unfair trade practices. Unhealthy, including concerning the right to privacy. In this function, the FTC has the authority to issue regulations, enforce specific privacy laws, take action in law enforcement, conduct company investigations, and resolve disputes. At the state level, the functions carried out by the FTC are carried out by the state attorney general's office. Almost the same model is applied in Canada, but in a more straightforward division, considering that the division is only separated into government, private, and state.

[50]Rosadi, S. D., & Pratama, G. G. (2018). "Urgensi Pelrindungan Data Privasi Dalam Era Ekonomi Digital Di Indonesia". *Veritas et Justitia, Vol.4. No.1,pg. 105*.
[51] Wahyudi Djafar M. Jodi Santoso, *Op. Cit.*, Pg. 10-11.

b. Dual Authority Model

The debate about the importance of protecting personal data often cannot be separated from the issue of information disclosure, as the opposite pole. This then affects the legislative model, which has implications for the supervisory authority model developed. As a result of this debate, in some countries some use the two-body model to separate it from other institutions with similar powers, such as the Ombudsman and the Information Commission. This model is widely adopted by European countries, such as Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Finland, France, Greece, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia. , Spain and Sweden. The choice of the two-agency model shows that between the two bodies for personal data protection and information disclosure, there are significant differences in terms of duties, roles, competencies, and authorities.

In this two-agency model, the concern is the potential for conflict between the two institutions. This situation results from two agencies or institutions operating on an issue that is closely related and simultaneously contradictory and can also negate each other. Even in practice, public debates between data protection agencies and information disclosure agencies cannot be denied, for example when dealing with cases that have a political dimension. In addition, there are also concerns that public bodies and individuals who have an interest will accept decisions or recommendations that conflict between the two bodies. Therefore, if two separate bodies exist, there must be a mechanism to resolve cases with different opinions or possible conflicts. There should be some form of a formal agreement to minimize conflict, such as a formal consultation process. The need for cooperation and synergy can be incorporated into the relevant legislation.

c. Single Authority Model

Considering efficiency and effectiveness, many countries have finally adopted a one-authority model to deal simultaneously with access to public information and protecting privacy. The countries that have formed this joint body are Germany (at the federal level), Switzerland (at the federal level), Ireland, Estonia, Serbia, England, Hungary, Slovenia, and Croatia.

In Europe, in general, data protection bodies developed into information commissions, but in the end, dozens of information commissions evolved into data protection bodies all at once. In Slovenia, for example, the information disclosure commission evolved into an information commission with the data protection inspectorate headed by an information commissioner. A similar model was also developed in Hungary, which added a data protection oversight function to the information commission, which was formed earlier in 2011.

The main benefit of establishing a single agency is that it can share and minimize differences of opinion between protecting personal data and information disclosure. Having one agency can also reduce the potential and the possibility of conflicts between institutions because in practice, many requests for information are under the jurisdiction of information disclosure law, which will later be related to personal information. Unifying the body with these two functions will allow for a better balance. It will also make it easier for the general public to have contact with public bodies so that they can make better use of their rights. Having one body can also trigger awareness. The better the two rights, the more awareness is raised for other public bodies. Creating a single body with two powers will also reduce the possibility of a public body abusing data protection. The weakness of the one-body model is that it allows for one interest that may be stronger or considered more substantial, so it fails to protect or balance the two interests in the dispute. In addition, any conflicts will tend to be decided internally

rather than publicly, resulting in less debate and less public control. There are also concerns that an agency may not be equipped with adequate resources to undertake additional tasks. Because in many cases, new functions added to an agency's mandate have resulted in additional work without the provision of adequate resources.

Some countries have chosen to have several independent supervisory authorities, namely:

a. France

Before the EU GDPR was promulgated in 1978, the French state had established a National Commission on Informatics and Freedom or Commission Nationale de l'Informatique et des Libertés (CNIL). This agency is an independent administrative authority as the national supervisory authority for the protection of personal data. CNIL is formed and performs its functions under the Law on Data, Documents and Freedoms. The independence of CNIL is guaranteed based on its composition and organization. The CNIL commissioners are made up of seventeen people, most of whom are elected by the legislature. CNIL elects a presiding officer from among its members and in the election does not receive any instructions from other authorities for the election of a chairman. The mandate of the commissioners is for five years.[52]

b. South Korea

The South Korean Personal Information Protection Commission (PIPC) was established under the Personal Information Protection Act 2011 (PIPA). PIPC is a collegial commission that carries out its role independently based on its mandate following PIPA. The position of the Personal Information Protection Commission is under the President but carries out its functions and authorities independently.

PIPC consists of 15 commissioners, one Chairman and one Permanent Commissioner, with the term of office of the Chairman and Commissioner being three years, and the term of office may be extended once. Filling the 15 Commissioners, namely five commissioners appointed from candidates selected by the National Assembly, five commissioners from candidates appointed by the Chief Justice of the Supreme Court, and five commissioners appointed by the President, taking into account people recommended by civil organizations or consumer groups related to privacy, associations trading consisting of personal information processors and other persons who have good academic knowledge and experience relating to personal information.[53]

c. Hongkong

The provisions of the Personal Data Privacy Ordinance (PDPO) of 1995 mandated the establishment of a Privacy Commissioner for Personal Data (PCPD) as an independent body tasked with overseeing and socializing compliance with the law. The function of the Personal Data Privacy Commissioner is comprehensive, including monitoring and supervising compliance with PDPO, providing socialization regarding public awareness and understanding of PDPO, examining proposed legislation so that the enactment of the legislation will not affect individual privacy, conducting inspections of personal data management systems, and conduct research on privacy matters. Hong Kong, requires third parties to manage data, either organizations or companies, to publish a privacy policy to the public. If violated, the Hong Kong government will provide a subpoena to the third party concerned.[54]

The commissioners of the PCPD consist of one Commissioner who serves for five years and has the right to be reappointed for no more than one term. The Chief Executive of Hong Kong appoints the Commissioner to carry out the functions and exercise the powers conferred by the Ordinance in protecting personal data privacy. The Commissioner may also resign from

[52]*Ibid.*, Pg. 15.
[53]*Ibid.*, Pg. 21.
[54] Greeneaf, Graham. 2014. Asian Data Privacy Laws-Trade and Human Rights Perspective. New York: Oxford University Press. p. 154.

his office by giving written notice to the Chief Executive or may be replaced by the Chief Executive with the approval of the Legislative Council on the grounds of inability to perform the functions of the PCPD or misconduct. The Chief Executive has the authority for the honorarium and the terms and conditions for the appointment of Commissioners. A person appointed as a commissioner is a civil servant, but he is not a government agency. In carrying out its functions, this commission has several divisions: Complaints Division, Compliance Division, Policy and Research Division, Legal Division, Communication and Education Division, and Corporate Inquiry and Support Division.[55]

d. Singapore

The Singapore Personal Data Protection Commission is known as the Personal Data Protection Commission (PDPC). This commission is attached to an existing institution, The Info-communications and Media Development Authority (IMDA). In 2012, IMDA was designated a Personal Data Protection Commission under the Info-Communications Media Development Authority Act No. 22 of 2016. The PDPC is formed by the relevant ministers whose membership is not less than six members and not more than 20 members. One of the commissioners other than the Chairperson or Deputy Chairperson may be appointed as the Chief Executive. In addition to appointing commissioners, the Minister may appoint one or more advisory committees to advise the Commission on personal data protection concerning implementing the Commission's duties and functions. In carrying out its duties, functions and authorities, the PDPC may consult with the advisory committee but is not bound by the results of the consultation or is independent.[56] The PDPC can regularly issue decisions relating to organizations that violate data protection provisions under the Personal Data Protection Act (PDPA). This commission also reminds individuals and organizations about their respective rights and obligations under PDPA.[57] In the long term, publishing cases on the PDPC website aims to promote and publicize inter-organizational accountability to protect consumer interest and trust.[58]

e. United States of America

Based on historical tracing, it was noted that the first country to regulate personal data protection was the state of Hesse in Germany in 1970, followed by Sweden in 1973, then the United States in 1974 and the United Kingdom in 1984. The United States, Australia, and Canada use the term personal information. In contrast, in the European Union countries, Malaysia and Indonesia itself, which is contained in the ITE Law, use the term personal data.[59] The United States of America is a country that implements the multi-supervisory authority model in data protection authority. One of the supervisory authorities in America is the Federal Trade Commission or Federal Trade Commission (FTC), which was established in the context of protecting consumer data in the trade and commercial sector. The FTC is a bipartisan federal agency with the dual mission of protecting consumers and promoting fair competition because initially, this agency was a business competition agency. Unfair or unhealthy business practices, including failure to implement reasonable security measures and violations of consumer privacy rights to the detriment of consumers in the states. In addition, various sector-specific regulators, particularly those in the healthcare, financial services, telecommunications and insurance sectors, have the authority to issue and enforce privacy and security regulations concerning entities under their jurisdiction. The FTC is led by five commissioners, nominated

[55]*Ibid*., Pg. 19.
[56]*Ibid*., Pg. 20.
[57] M. Yip, *"Personal Data Protection Act 2012: Understanding the consent obligation,"* Pers. Data Prot. Dig.2017, p. 266.
[58]W. B. Chik, *"The Singapore personal data protection act and an assessment of future trends in data privacy reform," Comput.Law Secur. Rev., vol.* 29, no. 5, 2013, p. 554.
[59]Lia Sautunnida,"Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia*", Kanun Jurnal Ilmu Hukum Vol. 20, No. 2, (Agustus, 2018), pg. 373.*

by the President and elected by the Senate to be appointed commissioners. Each commissioner has a term of office of seven years. Of the five commissioners, there are no more than three from the same political party. The chairman of the commissioners will be directly elected by the President, one of the five existing commissioners.[60]

Since the 1998 reformation, Indonesia has developed models of non-ministerial institutions that are independent, as well as state commissions or special agencies that are branches of executive branch agencies. Concerning personal data protection, the independent authority model is fundamental and most appropriate to enforce the Personal Data Protection Law. The personal data protection authority is not an extension of the ministry or executive but is a state institution that functions as an independent supervisor. The independence of the supervisory authority is very much needed, with a strong position and authority to oversee the implementation of the Personal Data Protection Law, both supervision of controllers and processors of personal data from the public (government) and private sectors. In addition, to ensure the fulfillment and protection of the rights of data subjects.[61]

As explained above, there are two policy options in the Personal Data Protection Act for establishing an independent supervisory authority in data protection. Such can be formed as a separate institution, such as Hong Kong and South Korea, or attached and add to the authority of existing institutions such as Singapore and the United States. The second option usually departs from considerations of efficiency, effectiveness, and acceleration of personal data protection. Suppose the choice is to attach the personal data protection authority to an existing institution. In that case, there is still a need to change the structure and composition of the commissioners and add to the duties and authorities of the existing institutions to ensure the independence of the commissioners who specifically handle data protection.[62]

As an illustration, referring to the practice in the United States, supervision of the protection of personal (consumer) data is given to the Federal Trade Commission (FTC), which in Indonesia has almost the same position and authority as the Business Competition Supervisory Commission (KPPU). A model such as the United States is only relevant if personal data protection laws are binding and apply to the commercial private sector. In Singapore, the Personal Data Protection Commission is attached to an existing agency, The Info-communications Media Development Authority (IMDA), which is an agency closely related to the communication and informatics governance function.[63]

As previously explained, there are many indicators to determine the independence of non-ministerial institutions, which function as supervisors for the protection of personal data, as applied by various models and countries described above. The European Union, for example, emphasizes that independence must at least be seen from institutional independence, independence of commissioners, independence of organizations, independence of human resources, and financial control must not affect independence.[64] This illustrates that if an independent supervisory authority is to be formed, it must be considered from the system, membership to financial sources of the authority so that an independent institution is genuinely formed.

Based on the existence of three independent supervisory authority models in the protection of personal data, namely the multiple authority model, the dual authority model, and the single authority model. Each has advantages and disadvantages. To ensure compliance with the

[60]*Ibid*., Pg. 14.
[61]*Ibid*., Pg. 24.
[62]*Ibid*., Pg. 24.
[63]*Ibid*., Pg. 24.
[64]*Ibid*., Pg. 25.

principles of personal data protection, a data protection authority is indispensable, either in the form of a single supervisory authority or its function attached to other independent institutions. Ideally, it is an independent institution that specifically handles personal data protection. However, by considering the efficiency and effectiveness of personal data protection, the supervisory authority function in data protection, for example, can be attached to other related institutions, such as the Information Commission or the Ombudsman, with the need to change the structure. The existing institutions.[65] For Indonesia, in establishing an independent supervisory authority, the choice of a single model is more suitable, namely by maximizing the existence of the Information Commission to manage not only public information disclosure but also handle personal data protection issues. This commission can work immediately because it has the same duties and functions the authorities must carry out.[66]

C. Conclusion

Based on the results of the study, it can be concluded:

1. The existence of an Independent Supervisory Authority in Indonesia in enforcing the Protection of Personal Data is essential, considering: first, there are considerations of independence, namely the amount of personal data processed by government data controllers or public bodies, so it is not easy to guarantee independence in supervision if the function is carried out by fellow government institutions. With an Independent Supervisory Authority, it is possible to monitor controllers and data processors from the private sector and public bodies (government). So that the supervision and enforcement are impartial and optimal. Second, there is a need to ensure the legal adequacy of Indonesia's data protection with other countries to implement the principle of extraterritorial jurisdiction of this law. Third, there is a consideration of checks and balances. The principle of independent authority will also provide convenience for data controllers in ensuring compliance and can protect and facilitate data subjects in making claims for their rights. Fourth, the existence of an independent supervisory authority can focus more on providing socialization of the regulations and interpreting the meaning of the applicable regulations to provide a good understanding and increase awareness in the community.
2. Based on three independent supervisory authority models for personal data protection, namely the multiple authority model, the dual authority model, and the single authority model. Each has advantages and disadvantages. Two policy options can be taken in the personal data protection law in Indonesia in establishing an independent data protection authority. That is, by being formed explicitly as a separate institution, such as Hong Kong and South Korea, or by attaching and adding to the authority of existing institutions such as Singapore and the United States. The second option can be considered as efficiency and effectiveness, as well as the acceleration of personal data protection.

The author suggests:

1. Accommodating the Independent Supervisory Authority provisions in the Bill on Protection of Personal Data.
2. Using a single model option and being attached to other related institutions such as the Information Commission with the need to change the existing institutional structure.

[65] Wahyudi Djafar M. Jodi Santoso, *Op.Cit.,*Pg. 24.
[66] Ahmad Budiman, *Op.Cit.,*pg. 27.

Bibliography

A. Book

Lawrence M. Friedman, 2009, System Hukum Dalam Perspektif Ilmu Sosial, *The Legal System: A Sosial Science Perspektive*, Nusa Media, Bandung, hlm 16. Diterjemahkan dalam buku Lawrence M. Friedman, 1969, *The Legal System: A Sosial Science Perspektive, Russel Soge Foundation, New York*.

Graham. Greeneaf. 2014. *Asian Data Privacy Laws-Trade and Human Rights Perspective. New York*: Oxford University Press.

Marzuki. Peter. Mahmud, *Penelitian Hukum*, (Jakarta: Kencana Prenada Media Group,2012).

Rosadi, S.D., 2015, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional*, Refika Aditama: Jakarta.

Wiranata, I Gede A.B., *Metode Penelitian Dan Penulisan Ilmiah Bidang Hukum*, (Bandar Lampung: Zam Zam Tower, 2017).

B. Journal

Amboro,F.Y.P,. Pusvita,P "Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia)", *https://journal.uib.ac.id/index.php/combine Volume 1 No 1. 2021.* https://journal.uib.ac.id/index.php/combines/article/view/4466

Budiman.Ahmad." Otoritas Pengawas Perlindungan Data Pribadi", *info singkat, Vol. XIII, No.5/I/Puslit/Februari/2021*.https://berkas.dpr.go.id/puslit/files/info_singkat/Info%20Singkat-XIII-5-I-P3DI-Maret-2021-181.pdf

Chassang, Gauthier, *"The impact of the EU general data protection regulation on scientific research"*, Ecancermedicalscience. 11:709, Januari 2017, doi: 10.3332/ecancer.2017.709, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5243137/ .

Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *"The European Union general data protection regulation: what it is and what it means",* Information & Communications Technology Law 2019, Vol. 28, No. 1,p. 85. https://doi.org/10.1080/13600834.2019.1573501.

Dewi, S. "Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia". *DEMO 2 JURNAL. 2016.* https://doi.org/10.20961/yustisia.v5i1.8712

Deanne. D.F.P., dan Fahrozi.M.H. Upaya Pencegahan Kebocoran Data Konsumen Melalui Pengesahan Ruu Perlindungan Data Pribadi (Studi Kasus E-Commerce Bhinneka.Com)", *Procceding: Call for Paper 2 nd National Conference on Law Studies: Legal Development Towards A Digital Society Era. 2020.* http://jurnal.borneo.ac.id/index.php/bolrev/article/view/2014/1429

Fanny Priscyllia,"Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum, *(JATISWARA), Vol. 34 No. 3 November 2019.* https://doi.org/10.29303/jatiswara.v34i3.218

Jeremias, Palito., Safira.A. S., & Tiara.A.R ,"Urgensi Pembentukan Pengaturan Perlindungan Data Pribadi Di Indonesia Serta Komparasi Pengaturan Di Jepang Dan Korea Selatan", *Supremasi Hukum, Volume 17 Nomor 1, Januari 2021.*

https://www.researchgate.net/publication/350435708_URGENSI_PEMBENTUKAN_PENGATURAN_PERLINDUNGAN_DATA_PRIBADI_DI_INDONESIA_SERTA_KOMPARASI_PENGATURAN_DI_JEPANG_DAN_KOREA_SELATAN

M. Yip, "Personal Data Protection Act 2012: Understanding the consent obligation*," Pers. Data Prot. Dig.2017. 10.2991/aebmr.k.200321.020*

Mahira, DF, Emilda YLisa NA, "Consumer Protection System (CPS): Siste, Perlindungan Data Pribadi Konsumen Melalui Collaboration Concept", *Legislatif, Vol.3 No.2, 2020.* https://journal.unhas.ac.id/index.php/jhl/article/view/10472

Mc Dermott, Yvonne*. "Conceptualising the right to data protection in an era of Big Data",* Big Data & Society, Sage Journal, January-June 2017. https://journals.sagepub.com/doi/pdf/10.1177/2053951716686994.

Nadiah Tsamara,"Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara*", Jurnal Suara Hukum, Vol. 3, No. 1, Maret 2021. https://journal.unesa.ac.id/index.php/suarahukum/article/view/11353/5957*

Natamiharja.Rudi and Stefany,"Perlindungan Hukum Atas Data Pribadi di Indonesia (Studi Terhadap Pelaksanaan Pelayanan Jasa Telekomunikasi PT. Telekomunikasi Selular)."*Prodigy Jurnal Perundang undangan, Mindoria,2019. https://scholar.google.com/citations?user=poUI-okAAAAJ&hl=id*

Padma Widyantari.., Sulistiyono.Adi,"Pelaksanaan Harmonisasi Rancangan Undang-Undang Perlindungan Data Pribadi (RUU PDP)", *Jurnal Privat Law Vol. VIII No. 1 Januari-Juni 2020. https://jurnal.uns.ac.id/privatlaw/article/download/40384/26564*

Purtova, Nadezhda, "*The law of everything. Broad concept of personal data and future of EU data protection law",* Law, Innovation And Technology, 2018 Vol. 10, No. 1. https://doi.org/10.1080/17579961.2018.1452176

Russel Butar,"Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia", Atlantis Press SARL, Advances in Economics, Business and Management Research, *Volume 130 3rd International Conference on Law and Governance (ICLAVE*), 2019.

Rahman.Faiz,"Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia", *Jurnal Legislasi Indonesia Vol 18 No. 1 - Maret 2021. https://e-jurnal.peraturan.go.id/index.php/jli/article/viewFile/736/pdf*

Rizal. Muhammad . Saiful. Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia", Jurnal Cakrawala Hukum, *Volume 10 No. 2 Desember 2019. https://doi.org/10.26905/idjch.v10i2.3349*

Rosadi, S. D., Pratama, G. G. "Urgensi Pelrindungan Data Privasi Dalam Era Ekonomi Digital Di Indone-sia". *Veritas et Justitia, Vol.4. No.1, 2018. https://www.academia.edu/49083339/PERLINDUNGAN_PRIVASI_DATA_PRIBADI_PERSPEKTIF_PERBANDINGAN_HUKUM*

Sandra Wachter, Brent Mittelstadt and Luciano Floridi, *"Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation,"* International Data Privacy Law, 2017, Vol. 7, No. 2, https://academic.oup.com/idpl/article/7/2/76/3860948.

Sautunnida. Lia ," Urgensi Undang-Undang Perlindungan Data Pribadi Di Indonesia; Studi Perbandingan Hukum Inggris Dan Malaysia", *Kanun Jurnal Ilmu Hukum Vol. 20, No. 2, (Agustus, 2018). https://doi.org/10.24815/kanun.v20i2.11159*

Sekaring. A. K ., & Andy U. W," Perlindungan Hukum Data Pribadi Sebagai Hak Privasi*", Alwasath Jurnal Ilmu HukumVolume 2 No. 1 April 2021. https://journal.unusia.ac.id/index.php/alwasath/article/download/127/113/*

Sinta Dewi,"Konsep Perlindungan Hukum Atas Privasi Dan Data Pribadi Dikaitkan Dengan Penggunaan Cloud Computing Di Indonesia", *Jurnal Yustisia, Vol. 15, No.1. 2016. https://jurnal.uns.ac.id/yustisia/article/download/8712/7802*

Sukawati.Ketut. Perbawati. Lanang Putra ," Konsep dan Prinsip Pengaturan Perlindungan Data Pribadi di Indonesia", *Prosiding Seminar Nasional FH UNMAS Denpasar "Urgensi dan Implikasi RUU Perlindungan Keamanan Kerahasiaan Data Diri Berbasis Digitalisasi".*

Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R. (2018). "Legal Protection for Urban Online-Transportation-User's Personal Data Disclosure in the Age of Digital Technology". *Padjadjaran Journal of Law, 5(3).2018. http://jurnal.unpad.ac.id/pjih/article/view/18908*

Upik Mutiara, Romi Maulana."Perlindungan Data Pribadi Sebagai Bagian Dari Hasak Asasi Mnusia Atas Perlindungan Diri Pribadi", *Indonesian Journal of Law and Policy Studies | Volume 1 No. 1 Mei 2020. http://dx.doi.org/10.31000/ijlp.v1i1.2648*

Y. McDermott, "Conceptualising the right to data protection in an era of Big Data*," Big Data Soc.*, vol. *4, no. 1, 2017. https://journals.sagepub.com/doi/full/10.1177/2053951716686994*

W. B. Chik, *"*The Singapore Personal Data Protection Act and An Assessment Of Future Trends In data privacy reform," Comput.Law Secure.Rev., *vol. 29, no. 5, 2013. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=3204&context=sol_research*

Wahyudi Djafar."Makalah disampaikan sebagai materi dalam kuliah umum "Tantangan Hukum dalam Era Analisis Big Data", *Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada, Yogyakarta, 26 Agustus 2019. https://law.ugm.ac.id/unduh-materi-kuliah-umum-tantangan-hukum-dalam-era-analisis-big-data/*

Wijaya. Glenn"Pelindungan Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum", *Law Review Volume XIX, Nomor 3 – Maret 2020. https://ojs.uph.edu/index.php/LR/article/view/2510/0*

C. Regulations

1945 Constitution of the Republic of Indonesia

Draft Law (RUU) on Personal Data Protection.

D. Internet

Budi Irawanto, "*Making It Personal: The Campaign Battle on Social Media in Indonesia"s 2019 Presidential Election"(*11 April 2019), https://iseas.edu.sg

https://www.dw.com/id/data-279-wni-bocor-desakan-uu-perlindungan-data-mencuat/a-57638257

https://kominfo.go.id/content/detail/15455/mengulas-tiga-klasifikasi-data-dalam-revisi-pp-pste/0/sorotan_media