CONSTITUTIONALE
Volume 3 Issue 1, January-June 2022: PP: 19-38.
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 Establishing Independent Supervisory Authority for Personal Data Protection in Indonesia

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 Bill 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 research 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 research uses a normative legal research method using a statutory approach, a conceptual approach, and a comparative approach. The results of this research 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 rapid advancement of information and communication technology (ICT) has brought about significant changes. While offering numerous opportunities, it also presents various challenges.[1] Indonesia, situated in the dynamic Asia Pacific region and among the most populous countries in Southeast Asia[2], exemplifies this trend. As reported by the general chairman of *APJII*, internet usage in Indonesia surged by 20-25% until June 2020 compared to 2018, with approximately 171.17 million users in a population of 264.14 million[3], positioning Indonesia as one of the world's foremost internet consumers.[4]

The internet serves as a pivotal medium for information dissemination and electronic communication, facilitating an array of services and products such as e-commerce, e-education, e-health, e-government, e-payment, social media, among others. [5] However, the pervasive use of internet technologies, primarily developed by private entities, raises concerns about privacy infringement and data misuse.[6] Government entities also rely on personal data for service provision and strategic planning in sectors like healthcare and education. Nonetheless, the indiscriminate collection of personal and customer data without explicit consent is becoming increasingly common.[7]

Passive collection of personal data through information technologies without consent poses a significant challenge. Safeguarding privacy rights and ensuring the protection of personal data are integral to upholding economic, social, and cultural rights. Neethling et al. highlight the importance of data protection, which involves legal safeguards against the processing of one's data by another party, typically the data controller.[8]

Regarding the protection of personal data, the Indonesian government has ratified the Covenant on Civil and Political Rights (ICCR) through Law No. 12 of 2005, affirming its commitment to safeguarding the privacy and personal data of its citizens. The right to privacy, inclusive of personal data protection, is enshrined as a constitutional right in CHAPTER XA Article 28A-28J of the 1945 Constitution of the Republic of Indonesia. Specifically, Article

[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 Research: 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.*

28G paragraph 1 of the Law guarantees the protection of personal data, family, honor, dignity, and property, emphasizing the fundamental human right to security against threats. [9]

Despite constitutional provisions, Indonesia currently lacks specialized legislation solely dedicated to personal data protection. Instead, regulations governing personal data protection are dispersed across various sectors, including the Telecommunications Law, *KIP* Law, ITE Law, Population Administration Law, Health Law, Banking Law, Human Rights Law, and Consumer Protection Law.[10] This fragmented regulatory landscape poses challenges in applying the legal principle of lex specialist in cases concerning personal data protection[11], as they may be subject to multiple laws and regulations.

The urgency of safeguarding personal data is escalating due to its potential misuse, which can violate the rights of data owners. Alarmingly, many individuals remain unaware of their privacy rights. This lack of awareness underscores the need for legislation mandating personal data protection. In 2021 alone, data breaches compromised the personal information of 279 million Indonesian citizens.[12] Consequently, the Personal Data Protection Bill (PDP) is currently queued for ratification under the 2021 Priority National Legislation Program (*Prolegnas*). This bill aims to establish legal frameworks ensuring privacy and personal data protection in Indonesia.[13]

Moreover, an analysis of personal data protection violations based on complaints reveals concerning trends. E-commerce accounts for 39.3% of reported violations, followed by public agencies at 14.3%.[14] Other significant contributors include fintech operators, consulting services, insurance, telecommunications, and social media platforms. This underscores the imperative of establishing an independent supervisory authority for personal data protection. Such an entity would oversee compliance across private institutions and governmental agencies, ensuring comprehensive supervision and enforcement.

Hence, establishing an independent supervisory authority for personal data protection is imperative to oversee various aspects of its implementation. During the Working Committee Meeting (*Panja*) of the Bill (*RUU*) on Personal Data Protection (PDP) between the Commission and the government, discussions revolved around the Problem Inventory List (*DIM*), including proposals from various factions regarding the formation of a supervisory authority for personal data protection. This authority would serve as the enforcer of the law, conducting investigations and imposing sanctions as necessary.

In the Personal Data Protection Bill *DIM*, the government outlines the role of the supervisory authority as the Data Protection Authority (DPA), responsible for overseeing compliance across private institutions and public or government agencies.[15] This entity plays a pivotal role not only in implementing privacy and data protection policies but also in raising awareness, providing consultation, and fostering network development. The DPA functions as an ombudsman, auditor, consultant, educator, policy advisor, and negotiator. Crucially, it must have the power to enforce the law, taking action against both private and public actors who violate data protection regulations.[16]

---

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

[10] 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.

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

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

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

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

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

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

The need for an independent supervisory authority to protect personal data is crucial for Indonesia, which currently lacks such oversight. Many countries already have independent institutions overseeing personal data protection, such as France, South Korea, Hong Kong, Singapore, Germany, and the United States.

The Personal Data Protection Bill, included in the 2021 Priority National Legislation Program, aims to address this gap. Discussions in the bill's working committee have focused on establishing regulations for an independent supervisory authority responsible for socialization, supervision, dispute resolution, mediation, and providing recommendations on personal data protection.[17]

This paper aims to analyze the urgency of establishing an independent supervisory authority in Indonesia, along with the ideal concept based on international comparisons. Using normative research methods[18], including statutory, conceptual, and comparative approaches[19], the author examines the mechanism and significance of such an authority in protecting personal data rights. The research contributes to the discourse on personal data protection and the role of supervisory authorities.

B. Discussion

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

Personal data encompasses various aspects of an individual's identity, such as their characteristics, name, age, gender, education, occupation, address, and familial status.[20] Warren and Brandeis argued that privacy is essential for individuals to enjoy life and have the freedom to be left alone, thus necessitating legal recognition and protection.[21] Van Der Sloot expanded this notion by including not only sensitive or private information[22] but also public and non-sensitive data within the scope of personal data.[23]

The right to privacy concerning personal data is enshrined as a constitutional right for Indonesian citizens according to the 1945 Constitution.[24] Indonesia's commitment to upholding this right is demonstrated through its ratification of the International Covenant on Civil and Political Rights (ICCPR) via Law Number 12 of 2005. This ratification aligns with Indonesia's constitutional acknowledgment of privacy rights, explicitly stated in Article 28G paragraph (1) and Article 28H paragraph (4) of the 1945 Constitution. These articles affirm the right to personal protection, property ownership, and security from undue intrusion or arbitrary seizure. In Indonesia, there are several regulations governing the protection of personal data, namely:[25]

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

[17]Ibid.
[18]I Gede A.B.Wiranata, *Metode Penelitian Dan Penulisan Ilmiah Bidang Hukum*, (Bandar Lampung: Zam Zam Tower, 2017), 60.
[19]Peter Mahmud Marzuki, *Penelitian Hukum*, (Jakarta: Kencana Prenada Media Group,2012), 93.
[20]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.*
[21]Rosadi, SD, 2015, *Cyber Law Aspek Data Privasi Menurut Hukum Internasional, Regional dan Nasional,* Refika Aditama: Jakarta, pg. 23.
[22]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.*
[23]Sekaring Ayumeida Kusnadi1 dan Andy Usmina Wijaya,"Perlindungan Hukum Data Pribadi Sebagai Hak Privasi", *Aiwaath Jurnal Ilmu HukumVolume2No. 1April202, pg. 11.*
[24]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.*
[25]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.*

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

There is disharmony among some of these regulations, making it challenging to apply 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 establish legal unification to regulate personal data protection, transforming what was previously spread across various sectors into a comprehensive and concurrent arrangement.[26] Apart from the rules regarding the protection of personal data across various laws and regulations, another crucial factor is the number of cases involving misuse of personal data and the unclear sanctions for perpetrators who steal or sell personal data. These factors serve as impetus for the Government and the House of Representatives to initiate the formulation of the Personal Data Protection Bill (*RUU* PDP).[27]

Although the Personal Data Protection Bill has not yet been ratified and promulgated, discussions in the Working Committee Meeting (*Panja*) of the *Bill* (*RUU*) on Personal Data Protection (PDP) between Commission I and the government revolved around the Problem Inventory List (*DIM*), including proposals from several factions regarding the establishment of a personal data protection supervisory authority to oversee the implementation of the law.[28] Following extensive reform, the European Union (EU) adopted a new Regulation (EU) on 27 April 2016 concerning the protection of individuals with respect to the processing of general personal data, known as the General Data Protection Regulation (GDPR). The GDPR introduces a new system based on a risk-based approach, implemented through an integrated data protection system that closely involves the data controller and processor and can adapt to various processing contexts.[29] "Personal data" is a critical notion in data protection law, determining the material scope of the Data Protection Directive (DPD) and the GDPR. Data protection principles, rights, and obligations apply only when personal data is processed (Article 3(1) DPD and Article 2(1) GDPR).[30]

The primary objective of any regulation on personal data is to mitigate privacy risks, specifically the occurrence of personal data breaches. These breaches are defined as security incidents leading to the destruction, loss, alteration, unauthorized disclosure, or access to personal data that is sent, stored, or otherwise processed. Personal data breaches, if not handled promptly and appropriately, can result in physical, material, or non-material harm to individuals. This harm may include loss of control over personal data, infringement of rights, discrimination, identity theft, fraud, unauthorized disclosure of pseudonyms, damage to

[26]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.*
[27] Glenn Wijaya,"*Pelindungan Data Pribadi Di Indonesia: Ius Constitutum Dan Ius Constituendum*", Law Review Volume XIX, Nomor 3 – Maret 2020, pg. 329.
[28]Ahmad Budiman, *Op. Cit*., pg. 26.
[29]Gauthier Chassang*,"The impact of the EU general data protection regulation on scientific research"*, Ecancermedicalscience. Januari 2017, 11: 709, p.79.
[30] 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.

reputation, loss of confidentiality of personal data protected by professional secrecy, or other significant economic or social losses.[31]

The GDPR outlines three possible legal grounds for the right to an explanation of automated decision-making. This right to explanation may be obtained from safeguards against automated decision-making as required. These bases are derived from (i) security, (ii) notification duties, and (iii) access rights, respectively. Overall, the assertion that the GDPR grants a right to an ex-post explanation of certain (minimum) decisions, applicable to any instance of automated decision-making, is based on a combination of protection and notification duties.[32]

Several principles of personal data protection are fundamental, including:[33]

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.[34]

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.[35]

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.

---

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

[32] 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.

[33] 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.

[34] 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.*

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

To safeguard personal rights rooted in fundamental principles, Indonesia requires an autonomous supervisory body dedicated to safeguarding personal data. This independent authority not only serves to oversee the implementation of personal data protection within society but also aims to catalyze behavioral shifts across all sectors involved in safeguarding personal data. It must possess the authority to monitor both private and public entities, including executive, legislative, and judicial bodies.[36]

An independent data protection authority ensures adherence to relevant laws and regulations by controllers and processors of personal data, be they individuals, private entities, or public institutions. This institution serves as a pivotal player in privacy and data protection, spearheading regulatory efforts through policy oversight, awareness campaigns, consultation, and network building. It hinges upon institutional autonomy, skilled human resources, and a clear delineation of roles and powers, insulated from personal or political influences.[37]

In essence, this autonomous body is tasked with supervising, monitoring, and enforcing personal data protection laws. Equipped with investigative capabilities, it can probe complaints, issue binding directives, levy penalties for infractions, and demand information from data controllers or processors. Moreover, it possesses auditing powers and the authority to access all pertinent information, including physical premises or equipment involved in data processing, if necessary.[38]

Ensuring the efficacy and success of the legal system requires attention to three legal components: legal structure, legal substance, and legal culture[39], as articulated by Lawrence M. Friedman. The structural component, particularly the court system, is vital in establishing an effective legal framework for information technology. The presence of an independent authority fosters an impartial and efficient enforcement structure. The substantive aspect pertains to the legislative content, encompassing the formulation of robust laws governing data protection, including:[40]

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.

Currently, judicial decisions on privacy violations rely heavily on individual beliefs and interpretations, leading to a lack of consensus. This underscores the need for regulations that can adapt to evolving circumstances, especially in the realm of information technology law. Legal culture plays a crucial role in shaping a responsive legal system, influenced by the community's perception of law and the traditions governing societal life. In Indonesia, the legislative process involves input from relevant departments and community feedback, reflecting the nation's legal culture.[41]

The urgency of the ratification of the Personal Data Protection Bill should consider several aspects as follows.

a. Independency

Establishing an independent authority is crucial as it oversees both private sector data controllers and processors as well as those of public bodies, ensuring impartiality and

[36] *Ibid.*
[37] Ahmad Budiman, *Op.Cit.,* Pg. 27.
[38] *Ibid., pg 28.*
[39] Lawrence M.Friedman, (1977), Law and Society, an introduction, Prentice H.l, New Jersey, h. 35.
[40] 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.
[41] 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.*

effectiveness in supervision and enforcement. When establishing such an authority, attention must be given to its level of independence. Article 52 of the EU GDPR outlines five key prerequisites for the independence of a personal data protection authority as follows.[42]

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.

To ensure genuine independence, the establishment of an autonomous supervisory body necessitates careful consideration. This entails safeguarding against governmental or executive influence. Primarily, the data protection authority is tasked with functioning as a supervisory agency, empowered to enforce compliance without infringing upon data protection regulations. Its mandate encompasses overseeing both private entities and public institutions, including executive, legislative, and judicial bodies, in upholding personal data protection standards.

b. Adequacy

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:

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

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

In Indonesia, personal data protection is addressed by multiple regulations, including Law Number 23 of 2006 on Population Administration amended by Law Number 24 of 2013, Government Regulation Number 71 of 2019 on Electronic Systems and Transactions, Ministerial Regulation Number 20 of 2016 on Personal Data Protection in Electronic Systems, and Ministerial Regulation Number 4 of 2016 on Information Security Management Systems. These regulations underscore Indonesia's commitment to protecting individuals' data.[43] However, the proliferation of data protection provisions across various statutes leads to inconsistencies in legal application. To address this, there is a pressing need for legal harmonization and system enhancement, notably through the establishment 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:[44]

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.
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.

[43] 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)

[44]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.

Following the EU GDPR's provisions, the necessity for an independent supervisory authority in safeguarding personal data is evident. To align with global standards and ensure Indonesia's recognition as a nation committed to equitable personal data protection, the establishment of such an authority is imperative. Thus, Indonesia can attain parity with the European Union and other recognized countries in this regard, garnering acknowledgment from the United Nations. This recognition offers numerous benefits for Indonesia, including fostering robust cooperation with other nations in enforcing personal data protection laws. Given the prevalence of cross-border data flows in today's digital and industrial landscape, countries need to attain adequate recognition to facilitate reasonable cooperation. Notable examples of countries meeting adequacy standards include Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Switzerland, Uruguay, Israel, Japan, Jersey, New Zealand, and the United States of America.

c. Check and Balance

The presence of an independent supervisory authority yields significant benefits by bridging gaps and minimizing discrepancies between the dual functions of personal data protection and information disclosure. This authority serves to mitigate potential inter-institutional conflicts, as many requests for information governed by disclosure laws often involve personal data. Therefore, addressing this issue is paramount. By consolidating entities or institutions responsible for these functions, a more harmonious balance can be achieved, facilitating improved public engagement with governmental bodies and enabling better exercise of rights. Essentially, this independent supervisory authority acts as a mediator between data controllers and data subjects.[45]

Moreover, it is crucial to delineate between data controllers and data processors, as underscored by the GDPR. Data controllers bear the primary responsibility for data, with stricter obligations imposed on processors. Some entities may attempt to evade privacy responsibilities by labeling themselves as "processors" while essentially functioning as controllers. Principally, controllers must furnish the Data Protection Authority with comprehensive information to demonstrate prudent and lawful actions. These records should detail the processing of personal data, including the purposes, access, duration of storage, and implemented security measures.[46]

d. Information Dissemination

Personal data protection violations have been on the rise, with complaints highlighting various sectors as contributors to breaches. Based on classifications, E-commerce tops the list, accounting for 39.3% of reported violations, followed by public agencies at 14.3%, fintech operators at 10.7%, consulting services at 7.1%, insurance at 7.1%, and telecommunications at 7.1%. Social media platforms and other sectors also contribute to the tally, comprising 3.6% and 10.8%, respectively. Notably, E-commerce stands out as the primary contributor to personal data breaches from 2019 to May 2021.

The growing reliance on information and communication technology has given rise to various criminal activities, posing tangible and intangible risks to individuals. The proliferation of internet usage has exacerbated the severity of personal data protection issues, heightening the risk of data leaks. Significant breaches include the theft of personal data from 25 million Telkomsel customers in 2011 and subsequent incidents such as the passenger data leak from Lion Air and Batik Air airlines, affecting tens of millions of individuals. This leaked data,

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

[46] 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.

including Identity Card (*KTP*) and passport numbers, accessed via Amazon Web Services (AWS) cloud computing, poses a substantial risk of misuse, leading to identity theft and fraud. This threat is particularly alarming given the ongoing shift towards a digital economy driven by creativity. For businesses, personal data is indispensable, as highlighted by Norton Report 2013, which indicates an alarming increase in cybercrime potential and risk in Indonesia, as reported by the Indonesia Security Incident Response Team on Internet Infrastructure's official website.[47]

The lack of public awareness regarding personal data protection and privacy rights necessitates proactive socialization efforts, including structuring protection activities, overseeing execution, and mediating disputes. An independent authority could play a pivotal role in disseminating information, elucidating regulatory interpretations, and enhancing public comprehension to mitigate potential misuse of personal data.[48] Despite existing ministries' socialization tasks, their broad responsibilities across various laws and regulations highlight the need for a specialized authority solely focused on personal data protection.

The inclusion of an Independent Authority in the Personal Data Protection Bill is crucial, delineating its tasks, functions, and powers to address the comprehensive scope of the law applicable to both private and public entities. Such an authority ensures supervisory independence, aligns with extraterritorial jurisdiction principles, and facilitates legal adequacy of Indonesian personal data protection vis-à-vis other countries. Embracing the single authority principle fosters compliance for data controllers and bolsters data subjects' rights while concentrating efforts on socializing regulations and interpreting their implications for enhanced regulatory understanding and compliance.

2. The Ideal Independent Supervisory Authority in the Protection of Personal Data in Indonesia

The European Union safeguards personal data privacy as a fundamental right under The European Union Charter of Fundamental Rights, enforced through legislation such as The General Data Protection Regulation (GDPR). This regulation represents a commitment to upholding citizens' rights in the digital age. Additionally, The European Union has established The Police Directive to supervise and protect citizens regarding personal data processing, imposing sanctions for violations against data owners. The GDPR standardizes data protection rules across EU countries[49], incorporating principles like the existence of an independent supervisory authority. Before examining the implementation of independent supervisory authorities in other nations, various models of data protection authorities applied in various countries are explained in the following section.[50]

a. Multi Authority Model

Some countries, such as the United States and Canada, employ a multi-agency approach to monitor personal data protection through various laws and policies. In the United States, there exists a complex network of federal and state-level regulations governing privacy and personal data protection, including notable legislation like the California Consumer Privacy Act of 2018 (CCPA). These regulations necessitate supervision from numerous institutions, particularly in the private sector, where the Federal Trade Commission (FTC) plays a central role as an independent regulatory agency established since 1914. The FTC oversees companies to safeguard consumers from unfair trade practices, including violations of privacy rights. It holds authority to issue regulations, enforce privacy laws, conduct investigations, and resolve

[47]Fanny Priscyllia, *Op.Cit.,*pg. 241
[48]Ahmad Budiman, *Op.Cit*.,pg 30.
[49]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.*
[50] Wahyudi Djafar M. Jodi Santoso*, Op. Cit.,* Pg. 10-11.

disputes. At the state level, similar functions are often carried out by the state attorney general's office. Canada follows a comparable model, albeit with a more straightforward division among government, private, and state sectors.

b. Dual Authority Model

The debate surrounding personal data protection often intertwines with issues of information disclosure, creating a legislative model that influences the development of supervisory authorities. Some countries have adopted a two-body model to separate these functions from other institutions with similar powers, such as the Ombudsman and the Information Commission. This model is prevalent in European countries like Austria, Belgium, Bulgaria, and others, where distinct agencies oversee personal data protection and information disclosure, each with specific duties, roles, competencies, and authorities.

However, the two-agency model raises concerns about potential conflicts between these institutions, given their close yet contradictory relationship. Public debates and conflicts may arise, particularly in cases with political dimensions, where decisions or recommendations may clash. To mitigate these conflicts, mechanisms must be established to resolve cases with differing opinions. Formal agreements or consultation processes can help minimize conflicts, ensuring cooperation and synergy between the two bodies while addressing potential conflicts in relevant legislation.

c. Single Authority Model

Taking into account efficiency and effectiveness, several countries have now embraced a unified authority approach to simultaneously address public information access and privacy protection. These nations include Germany (at the federal level), Switzerland (at the federal level), Ireland, Estonia, Serbia, England, Hungary, Slovenia, and Croatia. Across Europe, data protection bodies have transformed into information commissions, and eventually, numerous information commissions have consolidated into data protection bodies. For instance, in Slovenia, the information disclosure commission evolved into an information commission with the inclusion of a data protection inspectorate, overseen by an information commissioner. Hungary similarly adopted a model in 2011, integrating data protection oversight into its existing information commission.

The primary advantage of establishing a singular agency is its capacity to harmonize differing perspectives on safeguarding personal data and facilitating information disclosure. This consolidation reduces potential conflicts among institutions, as many information requests fall under both information disclosure and personal data protection laws. By unifying these functions, a more balanced approach is achieved, enhancing public engagement with governmental bodies and promoting awareness of individual rights. Furthermore, consolidating these functions mitigates the risk of data protection abuses by public entities. However, the single-agency model has its drawbacks. It may prioritize one interest over the other, potentially undermining the protection or equilibrium of both interests in disputes. Additionally, internal resolution of conflicts may limit public discourse and oversight. Concerns also arise regarding the agency's capacity to handle additional responsibilities without adequate resources, as the inclusion of new functions often increases workload without corresponding resource allocation. Some countries have established independent supervisory authorities, including:

a. France

Before the enactment of the EU General Data Protection Regulation (GDPR) in 1978, the French government had established the National Commission on Informatics and Liberty, known as the *Commission Nationale de l'Informatique et des Libertés* (*CNIL*). This agency serves as an independent administrative authority and acts as the national supervisory body for

safeguarding personal data. *CNIL* operates under the framework of the Data, Documents, and Freedoms Law. Its independence is ensured through its composition and structure, with seventeen commissioners, most of whom are appointed by the legislature. The election of *CNIL*'s chairperson is conducted autonomously, without influence from external authorities, and commissioners serve a five-year term.[51]

b. South Korea

The South Korean Personal Information Protection Commission (PIPC) was established under the Personal Information Protection Act of 2011 (PIPA). Functioning as a collegial commission, PIPC operates independently according to its mandate outlined in PIPA. Although positioned under the President, the commission executes its duties and exercises its authorities autonomously.

PIPC comprises 15 commissioners, including one Chairman and one Permanent Commissioner, each serving a three-year term with the possibility of extension once. The composition of the commission involves the appointment of five commissioners by the National Assembly, five by the Chief Justice of the Supreme Court, and five by the President. Consideration is given to candidates recommended by civil organizations, consumer groups focused on privacy, associations of personal information processors, and individuals with substantial academic expertise and experience in personal information matters.[52]

c. Hongkong

The enactment of the Personal Data Privacy Ordinance (PDPO) in 1995 mandated the establishment of the Privacy Commissioner for Personal Data (PCPD) as an independent entity tasked with overseeing and promoting compliance with the law. The role of the Privacy Commissioner encompasses various functions, including monitoring and supervising PDPO compliance, fostering public awareness and understanding of PDPO through educational initiatives, reviewing proposed legislation to safeguard individual privacy, conducting inspections of personal data management systems, and conducting research on privacy issues. In Hong Kong, organizations or companies handling data are required to publicly disclose a privacy policy, with violations subject to government subpoenas.[53]

The PCPD comprises a single Commissioner serving a five-year term, with the possibility of one term renewal. Appointed by the Chief Executive of Hong Kong, the Commissioner is responsible for upholding the Ordinance's provisions in safeguarding personal data privacy. The Commissioner may resign by providing written notice to the Chief Executive or be replaced with Legislative Council approval on grounds of incapacity or misconduct. The Chief Executive determines the honorarium and terms of Commissioners' appointments. While Commissioners are civil servants, the PCPD operates independently. The commission carries out its functions through various divisions, including Complaints, Compliance, Policy and Research, Legal, Communication and Education, and Corporate Inquiry and Support.[54]

d. Singapore

The Personal Data Protection Commission (PDPC) in Singapore operates within the structure of the Info-communications and Media Development Authority (IMDA). IMDA was designated as the Personal Data Protection Commission in 2012 under the Info-Communications Media Development Authority Act No. 22 of 2016. The PDPC comprises relevant ministers, with membership ranging from six to twenty members. The Chief Executive may be appointed from among the commissioners, excluding the Chairperson or Deputy

[51] *Ibid.,* Pg. 15.
[52] *Ibid.,* Pg. 21.
[53] Greeneaf, Graham. 2014. Asian Data Privacy Laws-Trade and Human Rights Perspective. New York: Oxford University Press. p. 154.
[54] *Ibid.,* Pg. 19.

Chairperson. Additionally, the Minister has the authority to establish advisory committees to provide guidance on personal data protection matters. While the PDPC may consult with these committees, it maintains independence in carrying out its duties and functions.

The PDPC has the authority to issue decisions regarding organizations found to violate data protection provisions outlined in the Personal Data Protection Act (PDPA) .[55] It also educates individuals and organizations about their rights and obligations under the PDPA.[56] By publishing cases on its website, the PDPC aims to promote and publicize inter-organizational accountability, safeguarding consumer interests and trust in the long run.[57]

e. United States of America

The first country to enact regulations on personal data protection was the state of Hesse in Germany in 1970, followed by Sweden in 1973, the United States in 1974, and the United Kingdom in 1984. While the United States, Australia, and Canada utilize the term "personal information," the European Union countries, Malaysia, and Indonesia, as stipulated in the ITE Law, employ the term "personal data." The United States of America employs a multi-supervisory authority model for data protection. Among its supervisory authorities is the Federal Trade Commission (FTC), established initially to safeguard consumer data in trade and commercial sectors. As a bipartisan federal agency, the FTC's dual mission is to protect consumers and foster fair competition, having originated as a business competition agency. It addresses unfair or detrimental business practices, including failure to implement reasonable security measures and violations of consumer privacy rights. Moreover, various sector-specific regulators, particularly in healthcare, financial services, telecommunications, and insurance, possess the authority to enforce privacy and security regulations within their respective jurisdictions.

The FTC is governed by five commissioners nominated by the President and appointed by the Senate. Each commissioner serves a seven-year term, with no more than three commissioners belonging to the same political party. The President directly elects the chairman from the existing commissioners.[58]

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.[59]

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.[60] Suppose the choice is to attach the personal data protection authority to an existing institution.

[55]*Ibid.,* Pg. 20.
[56] M. Yip, *"Personal Data Protection Act 2012: Understanding the consent obligation,"* Pers. Data Prot. Dig.2017, p. 266.
[57]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.
[58]*Ibid.,* Pg. 14.
[59]*Ibid*., Pg. 24.
[60]*Ibid.,* Pg. 24.

P-ISSN 2723-2492
E-ISSN 2745-9322

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. 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.[61]

As previously discussed, various indicators determine the independence of non-ministerial institutions acting as supervisors for personal data protection, as observed in different models and countries. The European Union, for instance, stresses the importance of institutional independence, commissioner independence, organizational independence, human resource independence, and financial control that does not compromise independence.[62] This underscores the need to carefully consider the system, membership, and financial sources of any independent supervisory authority to ensure its genuine independence.

Considering the existence of three models for independent supervisory authorities in personal data protection—the multiple authority model, the dual authority model, and the single authority model—each presents its own strengths and weaknesses. To uphold the principles of personal data protection effectively, a data protection authority is essential, whether as a single supervisory body or integrated into other independent institutions. Ideally, this would be an independent institution solely dedicated to personal data protection. However, for the sake of efficiency and effectiveness, the function of supervisory authority in data protection can be delegated to related institutions like the Information Commission or Ombudsman, necessitating adjustments to their existing structures.[63]

For Indonesia, adopting a single model appears more suitable, particularly by leveraging the Information Commission to manage not only public information disclosure but also address personal data protection issues. This approach enables swift action as the commission already possesses the necessary duties and functions required for such oversight.[64]

C. Conclusion

Based on the results of the research, it several conclusions were drawn as follows.

1. The presence of an Independent Supervisory Authority is crucial in Indonesia to enforce Personal Data Protection for several reasons. Firstly, concerns regarding independence arise due to the significant amount of personal data processed by government data controllers and public bodies, making it challenging to ensure impartial supervision if carried out by fellow government institutions. With an Independent Supervisory Authority, monitoring of controllers and data processors from both the private and public sectors becomes feasible, ensuring impartial and optimal supervision and enforcement. Secondly, there is a necessity to align Indonesia's data protection laws with those of other countries to implement the principle of extraterritorial jurisdiction effectively. Thirdly, establishing an independent authority adheres to the principle of checks and balances, providing data controllers with clarity on compliance requirements while also enabling data subjects to assert their rights more easily. Fourthly, an independent supervisory authority can dedicate

[61] *Ibid.,* Pg. 24.
[62] *Ibid.,* Pg. 25.
[63] Wahyudi Djafar M. Jodi Santoso, *Op.Cit.,*Pg. 24.
[64] Ahmad Budiman, *Op.Cit.,*pg. 27.

more resources to socializing regulations and interpreting their implications, fostering better understanding and awareness within the community.

2. Indonesia has two policy options in its Personal Data Protection law for establishing an independent data protection authority, considering the three models of independent supervisory authorities: the multiple authority model, the dual authority model, and the single authority model. The first option involves explicitly forming a separate institution, akin to Hong Kong and South Korea. Alternatively, Indonesia can opt for the second option by integrating data protection authority into existing institutions, as seen in Singapore and the United States. The latter option may offer efficiency and effectiveness advantages, expediting the implementation of personal data protection measures.

Based on the results of this research, suggestions were formulated as follows.

1. Accommodating the Independent Supervisory Authority provisions in the Bill on Protection of Personal Data is urgent.
2. A single model option should be used and integrated to other related institutions such as the Information Commission with the need to change the existing institutional structure.

References

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

Bu*DIM*an.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 Research: 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 Research | 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

Bill (*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