### 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

### Keywords:
- Independent Supervisory Authority
- Personal Data Protection

### DOI:

https://doi.org/10.25041/constitutionale.v3i1.2535
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. With consideration of efficiency and effectiveness, in Indonesia 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. Indonesia is a developing country in the Asia Pacific region which is one of the most populous countries in Southeast Asia. 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. This makes Indonesia one of the largest internet users in the world. 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. Almost all people use internet technology developed by private parties who are very at risk of violating the privacy rights of someone's personal data. In addition, government agencies also need personal data to provide services and to plan the delivery of health care and education to citizens. However, more and more personal data and customer data are collected arbitrarily without the consent of the data subject.

Personal data is also collected passively through the use of information technology, without the consent of the data subject. 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. 

With regard to the protection of personal data, the Indonesian government has ratified the Covenant on Civil and Political Rights (ICCR) which was 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. 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 which 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." 

Even though it has been stipulated in the constitution, Indonesia does not yet have any special rules in the regulation of personal data protection. 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, Consumer Protection Law. So this makes it difficult to use the legal principle of lex specialist when there is a case that is general in nature 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 convergent 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 protection of personal data. Based on 2021 data, personal data leaks reached 279 million Indonesian citizens. For this reason, currently the Personal Data Protection Bill (PDP) is in the process of 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.

This is also considering the number of cases 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 largest percentage contributor to personal data breaches during 2019-May 2021. While the second largest contributor is public agencies. 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 supervision of various parties, both private institutions and public or government agencies.

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 supervision of various matters. 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 DIM of the Personal Data Protection Bill 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. The key 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.

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

Currently, the discussion of the Personal Data Protection Bill 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 the government to draw up a regulation that regulates the independent Personal Data Protection supervisory authority. Substantive analysis that 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.

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, It is carried out using a statutory approach, a concept approach, and a comparative approach.

17 Ahmad Budiman, Op. Cit., Pg. 27.
18 Rancangan Undang-Undang (RUU) tentang Perlindungan Data Pribadi.
19Ibid.
20I Gede A.B.Wiranata, Metode Penelitian Dan Penulisan Ilmiah Bidang Hukum, (Bandar Lampung: Zam Zam Tower, 2017), 60.
21Peter Mahmud Marzuki, Penelitian Hukum, (Jakarta: Kencana Prenada Media Group, 2012), 93.
The author examines the urgency of an independent supervisory authority in the protection of 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.

B. Discussion

1. The urgency of having an Independent Supervisory Authority in the protection of personal data in Indonesia

Personal data is data relating to a person's characteristics, name, age, gender, education, occupation, address, and position in the family. According to Warren and Brandeis stated that: "Privacy is the right to enjoy life and the right to be left alone and this development of the law was inevitable and demanded of legal recognition". Which means that privacy is a right for everyone to enjoy life and demands that their privacy be protected. Van Der Sloot also stated that the term personal data does not only include sensitive or private data, but includes public and non-sensitive data. 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.

Indonesia has ratified the ICCPR through Law Number 12 of 2005 concerning Ratification of the International Covenant on Civil and Political Rights. Thus it can be concluded that the Government of Indonesia firmly supports the efforts of the international community in order 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).

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:

- Constitutional Court Decision Number 006/PUU-I/2003
- Law Number 17 of 2007 concerning Long-Term National Plan Development 2005-2025
- Law Number 39 of 1999 concerning Population Administration
- Law Number 11 of 2008 concerning Information and Electronic Transaction

25 Sekaring Ayumeida Kusnadi1 dan Andy Usmina Wijaya,”Perlindungan Hukum Data Pribadi Sebagai Hak Privasi”, Aiaaath Jurnal Ilmu HukumVolume2No.1April202, pg. 11.
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 Protection of Personal Data in Electronic Systems.

From some of these regulations there are disharmony, this makes it difficult to use the legal principle of lex specialist when there is a case that is general in nature and can be subject to various laws and regulations. Therefore, it is necessary to have a legal unification that regulates the protection of personal data as a whole so that what was previously spread in various sectors becomes a comprehensive and convergent arrangement. Apart from the fact that there are so many rules regarding the protection of personal data in various laws and regulations, another factor that is quite crucial 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).

The Personal Data Protection Bill which 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.

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, both close to the data controller and processor, and capable of adapting to various processing contexts. “Personal data” is one of the key 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).

The main 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.\textsuperscript{33}

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, respectively. We will assess each one in turn. Overall, the claim that a right is granted by the GDPR 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.\textsuperscript{34}

In the protection of personal data, there are several principles of personal data protection as a basic right, among others:\textsuperscript{35}

a. Privacy
Privacy can be defined in various ways, for example as the right to 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, in practice, privacy is concept-based on people's perceptions of interests and benefits.\textsuperscript{36}

b. Autonomy
Everyone should have control over their own personal data. The principle of autonomy and the related focus on consent are 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 basic 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 clear affirmative action indicating consent to the processing of personal 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.\textsuperscript{37}

\textsuperscript{33} Gauthier Chassang, Op.Cit. p.79.
\textsuperscript{37} Yvonne McDermott, "Conceptualising the right to data protection in an era of Big Data", Big Data & Society, Sage Journal, January-June 2017, p. 3.
d. Non-diskrimination

The rights to personal data protection and non-discrimination interact in different ways and need to be increased in effectiveness. Regarding data processing technology, there are two complementary aspects of data protection and non-discrimination rights, namely 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 in 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 the implementation of personal data protection in the community, but 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 personal data, not only overseeing the private sector but also supervising the public sector, namely executive, legislative, and judicial bodies or institutions.38

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 regulators in the field of privacy and data protection. The agency's key role is not only in overseeing implementation of privacy and data protection policies, but also in awareness raising, consulting, and network development. It takes institutional independence, personal human resources, and functions and authorities from the personal and political domains.39 In summary, the duty of this independent authority is to 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, 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 be able to request information from data controllers or processors, perform audits, gain access to all information that may be needed for investigation purposes, including physical access to buildings or equipment used for processing if necessary.40

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.41 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. With the existence of an independent authority, it 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 include:42

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

38 Ibid.
39 Ahmad Budiman, Op.Cit., Pg. 27.
40 Ibid., pg 28.
41 Lawrence M. Friedman, (1977), Law and Society, an introduction, Prentice H.I, New Jersey, h. 35.
At this time, judges in resolving cases of violation of privacy are still based on beliefs and interpretations so that 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 created properly 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 formation of laws is carried out by the legislature at the suggestion of the relevant departments, through input from the community.43

For this reason, with regard to the urgency of the ratification of the Personal Data Protection Bill, at least there are several things that can be used as a basis for consideration, namely:

a. Independence

The establishment of this independent authority is important, considering that this institution not only supervises controllers and processors of data from the private sector, but also 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. Basically, in terms of 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:44

1) Institutional independence, each supervisory authority must act with full independence in carrying out its duties and exercising its powers in accordance with the law.
2) The independence of the commissioner, a member of the supervisory authority, in carrying out his duties and authorities in accordance with 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, and etc.
4) Independence of human resources, the state must ensure that each supervisory authority chooses its own staff who are 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 truly independent authorities and are not under the auspices of the government or the executive. In principle, the data protection authority is not only expected to function as a supervisory agency, but also 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. With the existence of an independent authority, it 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 With Regard To 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 confidential.
(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. However, the spread of personal data protection provisions in various regulations causes disharmony in the application of the law so that legal unification and system improvement are needed, one of which is by formulating the existence of an independent supervisory authority.

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

1) Personal data must be processed in a legal, fair and transparent manner, such as:
   a. Obtained in accordance with 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 for information transparency in terms of processing their personal data, the right to access information for the purpose of collecting personal data (contracts, controllers), the right to delete and correct his personal

---

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 processing personal 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 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 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 that are independent from external influences which can also serve as a forum for dispute resolution.

6) Compensation, liability and sanctions can see the regulatory model of the EU GDPR in particular Chapter VIII that for example the owner of personal data can ask for compensation to the controller and/or processor if his personal data is misused and processed not in accordance with 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 this requires adequate recognition for a country so that they can cooperate well with each other. Countries that are considered to have met the adequacy include Andora, Argentina, Canada, Faroe Island, Guernsey, Isle of Man, Switzerland, Uruguay, Israel, Japan, Jersey, New Zealand, United State 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 one 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.47

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, even stricter obligations on processors. This happens because in some companies try to evade privacy responsibilities by declaring themselves to be "processors" while engaging in decisions like 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 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.48

d. Sosialization

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 largest 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 serious and at risk of leakage of someone's personal data. The personal data burglary that occurred in 2011 was 25 million Telkomsel customers, 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 which can lead to several cases of criminal acts such as identity theft or fraud, especially considering the current modern economic development towards a digital economy based on creative economy. For business people, personal data is included as very important 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 show an increase, which is compiled from the official website of the Indonesia Security Incident Response Team on Internet Infrastructure.49

This happens because people do not know at all about their privacy rights. Lack of public awareness of the importance of protecting personal data and fulfilling the right to privacy for themselves.

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.50 In addition, with the existence of its own independent authority, this institution will be able to focus on socializing, such as explaining the interpretation of a regulation in order to increase understanding for the public 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.

49Fanny Priscyllia, Op.Cit., pg. 241
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 on the formation of new institutions, for reasons of efficiency. 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 is difficult to guarantee independence in supervision, if this function is carried out by fellow government institutions. The need to ensure the legal adequacy of Indonesian personal data protection with other countries, in order to implement the principle of extraterritorial jurisdiction of this law. In addition, the principle of single authority (independent) will also provide convenience for both 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 based on comparisons in other countries

The protection of privacy for personal data in the European Union has been regulated as a basic 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 basic 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 that is used as a standard data protection rule in European Union countries. 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 to first understand the models of data protection authorities in various countries, namely.

a. Mutli Authority Model

Some countries that apply this model in monitoring the protection of personal data are the United States and Canada. Multi-agency policies are influenced by legislative policies or the establishment of sectoral data protection rules, through several laws. 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. 25 state laws relating to data privacy and privacy, including the California Consumer Privacy Act of 2018 (CCPA).

The many regulations related to privacy and data protection in the United States have implications for the many institutions that function as supervisors for the implementation of 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 basically formed to monitor companies and protect consumers from unfair trade practices. unhealthy, including in relation to the right to privacy. In this

function, the FTC has the authority to issue regulations, enforce certain privacy laws and take
action in law enforcement, conduct company investigations, including resolving 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 also applied in Canada, but in a simpler division, considering
that the division is only separated into government, private, and state.

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 there are those who use the two-body model, to separate it from other
institutions that have 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 is the result of the existence of two agencies or institutions operating
on an issue that are closely related and at the same time 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 actually conflict between the two bodies.
Therefore, if there are two separate bodies, there needs to be a mechanism to resolve cases with
different opinions or possible conflicts. There should be some form of formal agreement to
minimize conflict, such as a formal consultation process. The need for cooperation and synergy
between the two can even 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 with access to public information and protection of privacy at the same
time. 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 there were dozens of information commissions that 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 the establishment of a single agency is that it can share and minimize
differences of opinion between the function of 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.
The unification of the body with these two functions will allow for a better balance. It will also
make it easier for the general public to have one contact with public bodies, so that they can
make better use of their rights. Having one body can also trigger awareness. The better of the
two rights, it will also raise awareness for other public bodies. The creation of a single body with two powers will also reduce the possibility of a public body to abuse data protection. The weakness of the one-body model is that it allows for one interest that may be stronger or considered stronger so that it fails to protect or balance the two interests in 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**

Prior to the promulgation of the EU GDPR, 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 chairman 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 5 years.\(^\text{53}\)

b. **South Korea**

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

PIPC consists of 15 commissioners, in which there is one Chairman and one Permanent Commissioner, with the term of office of the Chairman and Commissioner is 3 years, and the term of office may be extended once. Filling the 15 Commissioners, namely 5 commissioners appointed from candidates selected by the National Assembly, 5 commissioners from candidates appointed by the Chief Justice of the Supreme Court, 5 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.\(^\text{54}\)

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 very broad, 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, which requires third parties to manage data, either

\(^{53}\)Ibid., Pg. 15.

\(^{54}\)Ibid., Pg. 21.
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.\(^{55}\)

The commissioners of the PCPD consist of one Commissioner, who serves for 5 years and has the right to be reappointed for no more than one term. The Commissioner is appointed by the Chief Executive of Hong Kong to carry out the functions and exercise the powers conferred by the Ordinance in protecting the privacy of personal data. The Commissioner may also resign from 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, as well as 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 including: Complaints Division, Compliance Division, Policy and Research Division, Legal Division, Communication and Education Division, and Corporate Inquiry and Support Division.\(^{56}\)

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, namely 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 6 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 also appoint one or more advisory committees to provide advice to the Commission on personal data protection in relation to the implementation of 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.\(^{57}\) The PDPC can regularly issue decisions relating to organizations found to have violated data protection provisions under the Personal Data Protection Act (PDPA). This commission also serves to remind individuals and organizations about their respective rights and obligations under PDPA.\(^{58}\) In the long term, the publication of cases on the PDPC website aims to promote and publicize inter-organizational accountability to protect consumer interest and trust.\(^{59}\)

e. United States of America

Based on historical tracing, it was noted that the first country to regulate the protection of personal data 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 uses the term personal information while in the European Union countries, Malaysia and Indonesia itself, which is contained in the ITE Law, uses the term personal data.\(^{60}\) 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 actually established in the


\(^{56}\) Ibid., Pg. 19.

\(^{57}\) Ibid., Pg. 20.


\(^{60}\) 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.
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 originally 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, with respect to entities under their jurisdiction. The FTC is led by 5 commissioners, who are nominated by the President and elected by the Senate to be appointed as commissioners. Each commissioner has a term of office of seven years. Of the five commissioners, there are no more than 3 commissioners from the same political party. The chairman of the commissioners will be directly elected by the President, one of the five existing commissioners.61

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. With regard to personal data protection, the independent authority model is very important 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.62

As explained above, there are two policy options in the Personal Data Protection Act in the establishment of an independent supervisory authority in data protection. Such as can be formed specifically as a separate institution, such as Hong Kong and South Korea, or attached and add to the authority of existing institutions such as in Singapore and the United States. The second option usually departs from considerations of efficiency and effectiveness, as well as acceleration of personal data protection. If the choice is to attach the personal data protection authority to an existing institution, there is still a need to change the structure, composition of the commissioners, and add to the duties and authorities of the existing institutions, as part of ensuring the independence of the commissioners who specifically handle data protection.63

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). The choice of a model such as the United States is only relevant if personal data protection laws are solely 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.64

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 as 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

61 Ibid., Pg. 14.
62 Ibid., Pg. 24.
63 Ibid., Pg. 24.
64 Ibid., Pg. 24.
resources, and financial control must not affect independence.65 This is an illustration 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 truly 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 principles of personal data protection, the presence of a data protection authority is very necessary, either in the form of a single supervisory authority, or its function is attached to other existing 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 of the existing institutions.66 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 not only manage public information disclosure, but also handle personal data protection issues. This commission can work immediately, because it has the same duties and functions as what the authorities must carry out.67

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 very necessary, considering: first, there are considerations of independence, namely the amount of personal data processed by government data controllers or public bodies, so it is difficult to guarantee independence in supervision if the function is carried out by fellow government institutions. With the existence of 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 is impartial and optimal. Second, there is a need to ensure the legal adequacy of Indonesia’s personal data protection with other countries in order to implement the principle of extraterritorial jurisdiction of this law. Third, there is a consideration of checks and balances, where the principle of independent authority will also provide convenience for both 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 so as to provide a good understanding and increase awareness for 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. There are two policy options that can be taken in the personal data protection law in Indonesia in the establishment of an independent data protection authority. That is, by being specifically formed as a separate institution, such as Hong Kong and South Korea, or by attaching and adding to the authority of existing institutions such as in Singapore and the United States. The second option can

65Ibid., Pg. 25.
67 Ahmad Budiman, Op.Cit., pg. 27.
be considered as efficiency and effectiveness, as well as acceleration of personal data protection.

The author suggests:
1. Accommodating the provisions regarding the Independent Supervisory Authority 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.

Bibliography

A. Book


B. Journal


The Urgency of Independent ...

Yulia Neta, Agsel Awanisa, Melisa


C. Regulations

1945 Constitution of the Republic of Indonesia

Draft Law (RUU) on Personal Data Protection.
D. Internet


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