Jurnal Ilmiah Hukum dan Hak Asasi Manusia (JIHHAM)
Vol 4, No 1, 2024, 11-25 https://doi.org/10.35912/jihham.v4i1.2962

The Urgency of Establishing LPPDP as an Effort to Strengthen Personal Data Protection: A Comparison between Indonesia, Hong Kong and Singapore

Veris Yunanda[1*], I Gede AB Wiranata[2], Yennie Agustin[3], Rohaini Rohaini[4], Ahmad Zazili[5]
Lampung University, Lampung[1,2,3,4,5]
verisyunanda@gmail.com

Riwayat Artikel
Diterima pada 22 Februari 2024
Revisi 1 pada 18 Maret 2024
Revisi 2 pada 5 April 2024
Revisi 3 pada 26 April 2024
Disetujui pada 22 Mei 2024

Abstract
Purpose: The aim of this research is to analyze the urgency of establishing the LPPDP to strengthen personal data protection laws in Indonesia through a comparison of laws and practices in Hong Kong and Singapore, and to determine the opportunities and challenges of establishing the LPPDP in Indonesia.
Methodology: This study uses normative legal research methods with statutory, conceptual, and comparative approaches.
Results: The results show that the existence of an independent LPPDP will strengthen personal data protection law effectively and comply with an adequate level of protection with other developed countries. Thus, the President must immediately establish an LPPDP regarding the minimum requirements for the DPA's establishment in international practice.
Limitations: However, instead of achieving this noble goal, there are several recommendations that can be applied to establish the formation of LPPDP, whether in the form of a single supervisory authority or ministry based-model.
Contributions: Law Number 27 of 2022 concerning Personal Data Protection (UU PDP) has directly mandated the establishment of a data protection authority that was determined by the president. The LPPDP is projected to become an authority that acts as a supervisor and law enforcer for personal data protection in Indonesia, and it must be able to perform its functions, duties, and authorities independently.
Keywords: *Data Protection Authority, Independence, Personal Data Protection*
How to Cite: Yunanda, V., Wiranata, I, G, AB., Agustin, Y., Rohaini, R., Zazili, A. (2024). The Urgency of Establishing LPPDP as an Effort to Strengthen Personal Data Protection: A Comparison between Indonesia, Hong Kong and Singapore. *Jurnal Ilmiah Hukum dan Hak Asasi Manusia*, 4(1), 11-25.

1. Introduction

In the 4th paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia, it is stated that the Indonesian Government has a constitutional obligation to protect the entire Indonesian nation and all of Indonesia's blood and to promote general welfare, educate the life of the nation, and participate in implementing world order based on independence. Lasting peace and social justice. In the context of the development of information and communication technology, the goal of the state is realized in the form of protecting the personal data of every Indonesian resident or citizen (Kartika, Septiana, Ariani, Kasmawati, & Nurhasanah, 2022).

As a form of innovation, information technology is now capable of collecting, storing, sharing and analyzing data. These activities have resulted in various sectors of life utilizing information technology systems, such as the implementation of electronic commerce (e-commerce) in the trade/business sector, electronic education (e-education) in the education sector, electronic health (e-health) in the health sector, electronic government (e-government) in the fields of government, search engines, social

networks, smartphones and mobile internet as well as the development of the cloud computing industry (Arafat, 2015).

Information and Communications Technology (ICT) and digital transformation have radically changed the world balance. Currently, the presence of technology makes it possible to trace human behavior patterns. One of the biggest challenges resulting from digital transformation is in the aspect of privacy because in reality humans are now starting to share information and data as the most important part of big data connectivity, such as searching, collecting, investigating and analyzing behavior. This has the impact of expanding the scope of protection of privacy rights, which was previously limited to the real world, now also includes the virtual and electronic world (Sudaryanti, Darmawan, & Purwanti, 2013).

The concept of data protection implies that individuals have the right to determine whether or not they will share or exchange their personal data. In addition, individuals also have the right to determine the conditions for the transfer of personal data. Furthermore, data protection is also related to the concept of the right to privacy. The right to privacy has developed so that it can be used to formulate the right to protect personal data (Alim, 2023). The right to privacy through data protection is a key element for individual freedom and dignity. Data protection is a driving force for the realization of political, spiritual, religious and even sexual freedom. The right to self-determination, freedom of expression and privacy are rights that are important to make us human. The collection and dissemination of personal data is a violation of a person's privacy because the right to privacy includes the right to determine whether to provide or not provide personal data. Personal data is an asset or commodity of high economic value. In addition, there is a correlative relationship between the level of trust and the protection of certain data from private life.

Regulations regarding personal data protection will minimize the threat of misuse of personal data in the banking industry, online friendship sites (for example Facebook, My Space, Twitter, Path, Google Plus), electronic KTP (e-KTP) programs, e-health. The potential for crime to occur stems from searching for someone's personal data, removing the identity of data from criminals, search engine searches (eg google.com and bing.com), and cloud computing. By considering all the threats and potential violations above, personal data protection arrangements are intended to protect consumer interests and provide economic benefits for Indonesia (Aurora, Tisnanta, & Triono, 2023).

Potential privacy violations on social media do not only arise due to private sector practices, furthermore potential privacy violations can also arise from programs rolled out by the government with the involvement of private parties such as the electronic KTP (e-KTP) and e-health programs. In fact, based on leaked information from the Wikileaks cable, which contained a presentation by the British company ThorpeGlen, the observation method can be carried out using e-KTP. According to this information, by using the e-KTP device, citizens can track their whereabouts and activities. Utilizing this method, the state can easily observe the private lives of each of its citizens so that civil liberties are violated arbitrarily.

The implementation of e-KTP in Indonesia also faces various problems. These problems include the server used by e-KTP belonging to another country so that the data base in it is very vulnerable to being accessed by irresponsible parties . Then, the physical e-KTP vendor does not adhere to an open systemso the Ministry of Home Affairs cannot tamper with the system. Lastly, there have been many data base leaks. From several of these problems, it can be seen that the protection of people's personal data recorded on e-KTP is very vulnerable in terms of security. Potential violations in the e-KTP program also occur in the e-health program. In the future, the problem of protecting personal data will become more complicated, especially in the health service sector by implementing an e-health program which is being designed to be implemented simultaneously with the launch of the second generation e-KTP. The second generation e-KTP will later use a microchip to store the owner's data, including a list of people's health history. This electronic ID card will later be able to record people's health lists and history, making it easier for doctors to examine them and of course benefiting the community.

However, this program will be very dangerous if it is not supported by adequate regulations because it is feared that the privacy of patient personal data will not be protected so that it can be compiled, accessed and disseminated to other parties to be exploited economically by other service provider industries such as the pharmaceutical industry, insurance industry or other related industries. In the BPJS (Health Insurance Administering Body) program which is then integrated with the ASKES (Health Insurance) Program which includes personal health data of all Civil Servants, the Government has personal health data of patients and the public does not know how the BPJS program organizers will maintain the confidentiality of patient health data. This is very sensitive data.

It turns out that potential online violations such as those that occurred in the e-health program above also exist in offline settings, or those that do not use information technology. One of these offline violations is the misuse by companies of customers' personal data submitted as a requirement for business transactions, plus the potential for crimes that arise from searches for someone's personal data and the removal of the identity of data from criminals.

Another potential threat arises from the function of search engines on the internet. Search engines have long been used to help internet users by providing the widest possible information regarding the data available on the network. Search engines on the internet often expand their services to include email services, photo storage or even data storage. Thus, there is a threat that these additional services may allow search engines to intercept the information provided by users when registering to use the service.

One of the communication and information technologies that is developing rapidly at the moment is cloud computing technology. Cloud computing is a combination of the use of computer technology (computing) in a network with internet-based development (cloud). Currently, several leading information and communications technology companies have released applications to provide user data storage space such as Evernote, Dropbox, Google Drive, Sky Drive, Youtube, Scribd, iCloud, and so on.

The development of the use of this technology raises the potential for serious violations. An example of the latest violation is the breach of iCloud user data (cloud computing provided by Apple) which then spread to several mass media. This case received a lot of public attention because the data owners were several famous Hollywood celebrities, such as Jennifer Lawrence, Jenny McCarthy, Rihanna, Kate Upton, Mary Elizabeth Winstead, Kristen Dunst, Ariana Grande, and Victoria Justice.

The relatively large number of iCloud users has the potential to grow rapidly considering the current trend of Apple usage throughout the world, including in Indonesia. Referring to this, the potential for privacy violations currently in the field of cloud computing is very large. The increasing amount of data stored in the 'cloud' in the network (cloud), is a relatively new development. Additionally, when personal data is transmitted to the internet, the threat of risk arises as individuals lose control over that data. Once the data is stored in the cloud, another risk arises from the cloud service provider because it is possible for the cloud service provider to move information or data from one jurisdiction to another or from operator to another operator, or from one machine to another, without notification to the data owner.

By considering all the threats and potential violations that have been described, personal data protection arrangements are intended to protect consumer interests and provide economic benefits for Indonesia. This arrangement will protect individual personal data against misuse when the data has high value for business purposes, the collection and processing of which has become increasingly easier with the development of information and communication technology. The development of regulations on personal data protection in general will place Indonesia on par with countries with advanced economies, which have implemented laws regarding personal data protection. This will strengthen and strengthen Indonesia's position as a trusted business and investment center, which is a key strategy in Indonesia's economic development.

For consumer interests, the need to protect consumer personal data, especially in an era where personal data has become very valuable for business purposes, raises concerns that consumer personal data is being sold or used without consumer consent, as in the examples of violations described previously. Therefore, special personal data protection in a law is very necessary to ensure that consumers' personal data is properly protected. For economic development, special personal data protection will strengthen Indonesia's position as a trusted business and investment center and create a conducive environment for the growth of global data management and data processing industries such as cloud computing to develop in Indonesia. Regulations regarding personal data are very necessary because they regulate the collection, use, disclosure, transfer and security of personal data and in general the regulation of personal data is to find a balance between the need to protect individual personal data with the need for governments and business actors to obtain and process personal data for reasonable and legitimate needs (Hakim, 2019).

Referring to these conditions, after the ratification of Law Number 27 of 2022 concerning Personal Data Protection (hereinafter referred to as the PDP Law), there are various implementing provisions that must be followed up by the government. One of these provisions is the establishment of a personal data protection supervisory agency. The mandate of this law is contained in Article 58 Paragraph (2) of the PDP Law which has the authority to handle personal data protection issues (Akib, Triono, Tisnanta, & Medlimo, 2023). By having an institution that covers this problem, it will make it easier for the public if they want to get protection from crimes, such as data theft, hacking or misuse of personal data.

The existence of a personal data protection authority or institution is very important in order to ensure the effective implementation of the PDP Law which is carried out based on the principles, rules, processes and objectives of establishing the authority, as well as ensuring compliance by the public and private sectors with the principles and provisions of the personal data protection law. Apart from that, in the future this authority will be the spearhead of implementing policies that monitor and increase awareness of private actors and public authorities in efforts to protect personal data (Kartika & Medlimo, 2023). Not only that, because its existence is very necessary in a country, this authority must be equipped with authority, impartiality, and can be an institution that effectively monitors the implementation of the PDP Law in Indonesia. In the international scope, there are two known models of authority or personal data protection institutions, namely the authority model that exists independently and the authority that is under certain institutions such as ministries (ministry-based model).

The dynamics related to the regulation of personal data protection institutions have so far only been sectoral and not comprehensive, for example in the banking sector there is the Financial Services Authority (OJK), which has the authority to supervise banking customer data. Apart from that, there is the Ministry of Communication and Information (Kemenkominfo) and the National Cyber and Crypto Agency (BSSN) in the context of protecting people's personal data. It can be said that the implementation of data monitoring in the sectoral sector is not going well, as evidenced by the many cases of data leaks, both private and government data. The absence of a special institution that handles the protection of personal data can result in overlapping authorities, such as if there is a leak of government data, it is not known who is responsible, whether the Ministry of Communication and Information or BSSN, or even other parties (Khan & Sultana, 2021).

There are various tasks related to handling information security incidents, such as monitoring and handling hate speech which also involves the Ministry of Communication and Information and the Indonesian Police. Apart from that, the handling of cyber crime is handled by the National Police Headquarters Cybercrime Unit, and the Ministry of Defense which has a Cyber Operation Center (COC) for defense efforts. Financial crimes and the digital economy are handled by PPATK and KPK, and there may still be other overlapping tasks between these institutions. Following up on significant changes in the field of technology that have led to the emergence of various criminal acts that disrupt the social order of Indonesian society, this research will examine the Urgency of Establishing PPDP as an Effort to Strengthen Personal Data Protection: A Comparison between Indonesia, Hong Kong and Singapore as a form of law enforcement against cases of personal data leakage in Indonesia.

2. Literature Review

2.1 Practices of Personal Data Protection Supervisory Authorities in Hong Kong and Singapore

The regulation of privacy and personal data in Hong Kong is known as the Personal Data (Privacy) Ordinance (Cap 486) (PDPO) which was passed in 1995 and came into force in December 1996. PDPO applies to all user data, both the public sector and the private sector that controls, collect, store, process and use personal data (Privacy Commissioner for Personal Data Hong Kong (PCPD HK): 5). The independent supervisory authority in Hong Kong is known as the Privacy Commissioner for Personal Data (PCPD). PCPD was formed as an independent legal entity based on PDPO. Structurally, the PCPD is led by a Commissioner who is appointed directly by the Chief Executive of the Hong Kong Special Administrative Region (HKSAR). The PCPD is an independent statutory body established with the aim of overseeing enforcement and addressing compliance with the PDPO, receiving and processing complaints, and issuing guidance to the public and private sectors to comply effectively with the PDPO.

Privacy laws and personal data protection in Singapore are regulated based on the Personal Data Protection Act (PDPA). The privacy and personal data protection provisions in the Singapore PDPA do not apply to any government institution or public body. Because there are differences in the way of working between public institutions or legal entities and the private sector in Singapore, the public sector must comply with the Government Instruction Manuals and the Public Sector (Governance) Act (PSGA). Because the PDPA does not apply to the public sector, the supervision is different. Collectively, these public bodies are subject to high standards of responsibility with regular mandatory audits carried out to ensure that public bodies comply with personal data protection standards.

In practice in Singapore, the Personal Data Protection Commission (PDPC) is institutionally under the auspices of the Ministry of Communications and Information (MCI) which is part of The Info-communications and Media Development Authority (IMDA) as the main authority in charge of protection. personal data. Application of Strict Liability Principles to Environmental Dispute Resolution. Annals of Justice and Humanity, 2(2), 65-75.] PDPC was formed based on the Info-Communications Media Development Authority Act 2016—Act No. 22 of 2016 (Amendments to Personal Data Protection Act 2012). Explicitly, its institutional status is as a government authority and not an independent legal entity like the Hong Kong PCPD (Saputri, Rayi, Shafira Maya, Fardianyah Irzal, 2022). The PDPC model which is part of the ministry (ministry-based model) is very different from the independent model, especially because this greatly influences the legal adequacy of personal data protection in the country compared to other developed countries which apply adequacy rules and EU GDPR standards. This is because the PDPC's jurisdiction is only limited to the private sector and does not include the public sector.

Between these two forms of DPA, there are fundamental differences in terms of institutional independence and the appointment of commissioners. Hong Kong emphasizes that the PCPD's jurisdiction does not only apply to the private sector, but also the public sector because it was created as an independent legal entity. Meanwhile, PDPC Singapore does not have the power to supervise the actions of public or government legal entities like other DPAs and its jurisdiction only applies to the private sector.

In general, the institutions of personal data protection supervisory authorities between Hong Kong and Singapore can be compared as follows:

Element	Hongkong	Singapore
Institutional Model	PCPD was formed as an independent legal entity (independent supervisory authority) based on PDPO Hong Kong.	PDPC adheres to a ministry-based model, is attached to the Ministry of Communications and Information (MCI) and is part of The Info-Communications and

		Media Development Authority (IMDA) based on IMDA Act No. 22 of 2016.
Competence	Has authority over every person and all sectors that are data controllers and processors, including public and private bodies.	Only has authority over the private sector and individuals, does not have the competence to exercise authority over public institutions.
Filling Positions	The PCPD Commissioner is appointed directly by the Chief Executive of HKSAR with a term of office of 5 years and is entitled to be reappointed no more than once.	The PDPC Chief Executive is appointed by the IMDA authority with the approval of the MCI in prior consultation with the Public Service Commission.
Dismissal and Filling of Positions	The PCPD Commissioner may resign because: Submit your resignation in writing to the Chief Executive of the HKSAR Dismissed by the Chief Executive of the HKSAR with the approval of the Legislative Council if it is proven that there is an inability to carry out the functions as a commissioner and/or violates the provisions of the laws and regulations (misbehavior).	Dismissal and filling of the position of PDPC Chief Executive can only be carried out by the IMDA authority with the approval of the MCI in consultation with the Public Service Commission. Termination of office at any time and can be done without giving any reason.

Based on the table of institutional differences between PCPD and PDPC above, the PCPD commissioner is appointed directly by the Chief Executive of HKSAR with the dismissal and revocation of the commissioner's position regulated by clear conditions through the PDPO (Personal Data (Privacy) Ordinance Hong Kong, Cap. 486, Section 5 (5)). This mechanism for appointing and dismissing positions in the Hong Kong PCPD indicates that the PCPD is an independent state institution where the commissioner has a fixed position, meaning that someone appointed cannot quit at any time and can only be dismissed from their position with the provisions stipulated in the law that created it, not in a way determined by the President or in Hong Kong practice, namely by the Chief Executive.

Regarding the appointment of the Singapore PDPC commissioner, there are quite clear differences with the Hong Kong PCPD. According to PDPA Singapore, the authority with MCI approval can appoint a Chief Executive, including determining the termination of his position at any time and can do so without giving any reason (Info-Communications Media Development Authority Act 2016 (Act No. 22 of 2016), Section 40(3)). This of course emerged as a logical consequence of the limited rules and status given by PDPA Singapore to PDPC as an institution under The Info-Communications and Media Development Authority (IMDA).

As a consideration for Indonesia, there are two models of formation as existing in these two countries' practices. First, the formation of a single supervisory authority or single independent authority model as a special institution that uses the principle of single authority. Second, the ministry-based model, where the formation model is under the relevant agency such as the ministry. European countries that comply with the provisions of the EU GDPR require the establishment of an independent supervisory authority, so that almost 90% of countries in Europe that already have personal data protection laws choose this model.

Referring to Article 58 of the PDP Law, it is stated that the LPPDP is established and responsible to the President. The institutional model whose formation is determined and responsible to the President has been known in constitutional practice in Indonesia as a form of state auxiliary bodies (Medlimo, 2024). In the context of establishing a DPA, it must have a strong foundation by having to be formed as an independent legal entity that is free from all political elements, government control in making decisions, financial problems, and so on. There are several mechanisms and recommendations that are appropriate when looking at the practices of several countries in forming DPAs and can be applied in Indonesia in formulating an independent LPPDP organizational structure, leadership and staff in order to achieve equality and minimum DPA requirements.

First, the state institution model established for the LPPDP is as a supporting state institution under the executive, namely the President. The President can choose one of two institutional models known internationally, namely first, the LPPDP is formed as a state institution that is directly responsible to the President. Second, LPPDP was formed as a state institution that is responsible to the President through the relevant Minister (ministry-based model). Even though institutionally the LPPDP will be under the President, in reality there are currently a lot of user data from the public sector and considering the scope, function, duties and authority that the PDP Law provides is very broad, by adapting to these needs, the position of the LPPDP can be made possible. Even though it is in the executive branch, in carrying out its functions the LPPDP has independence.

The implementation of these two DPA institutional models actually still has gaps and concerns regarding ensuring the independence of the LPPDP. In the practice of the Hong Kong PCPD with a single supervisory authority and the Singapore PDPC with a ministry-based model, the fundamental difference between the practices of the two countries which use different DPA institutional models lies in their status and position. Where the Hong Kong PCPD was formed as a separate state institution, it has the status of an independent state institution appointed and directly responsible to the Chief of Executive of HKSAR. Meanwhile, in practice, PDPC Singapore, due to its formation as part of IMDA which is under MCI Singapore, its position is not as a state institution itself but as one of the commissions within IMDA which is appointed and responsible to the Minister.

These differences in institutional models also influence the recruitment and dismissal patterns of commissioners. Where in the practice of the Hong Kong PCPD, the mechanism for appointing commissioners is appointed by the Chief Executive of HKSAR with the terms and conditions regulated in the PDPO, including that the appointment must be made by the state gazette. Meanwhile, with the institutional model under a ministry, such as the practice of PDPC Singapore, the appointment of commissioners is carried out by the IMDA authority with the approval of the relevant Minister. This means that the process of filling the position of commissioner in PDPC Singapore is handed over to the Minister and IMDA in office and will always follow the political periodization of the relevant Minister. Likewise, in the case of dismissal from office, differences in institutional models also determine the dismissal mechanism which characterizes independence with a mechanism that is closely related to the policy (political will) that will be taken by a particular institution.

Apart from that, other differences exist in the scope of duties of the two DPAs. Where in the practice of the Hong Kong PCPD, with its own comprehensive PDPO regulatory model, meaning that it does not differentiate between regulations for each sector but reaches all public and private sectors, its supervisory authority also has the same scope with broad duties and authority to reach all sectors. Meanwhile, in Singapore's practice, the Singapore PDPA regulatory model only applies to the private

sector and organizations, so the PDPC can only carry out its duties and authority to private data controllers and processors. The scope of this authority in the future will greatly influence the capacity of a supervisory authority in carrying out its duties, functions and authority over data controllers and processors.

Ideally, the DPA is formed on the model of an independent state institution specifically related to the protection of personal data. However, along with the development and consideration of efficiency, effectiveness and acceleration of personal data protection, especially in developing countries, the ministry-based institutional model is also known. If in the future the formation of the LPPDP will implement a model under the ministry, it is feared that several independence qualifications as discussed previously will be difficult to fulfill. Therefore, in the formation of the LPPDP there is an urgency to form a structural design, commissioners, duties, functions and authorities that guarantee its independence as the main authority for protecting personal data in Indonesia which can freely and not be influenced by any party in carrying out supervision and law enforcement. public and private bodies.

Second, in relation to filling LPPDP positions, the President has the prerogative to appoint leaders based on the approval of the People's Representative Council (DPR). In order to avoid vested interests and maintain independence, filling positions cannot be done by direct appointment by just one political authority, at least the selection of commissioners must involve two public authorities, namely the President and the DPR (Rahma, Triono, & AT, 2023). In avoiding and minimizing political interests or certain closeness of the President or DPR, the commissioner recruitment process needs to be carried out transparently, with public involvement through the DPR, tightening the rules and selection preferences based on the criteria that have been regulated in the regulations establishing the LPPDP and not determined by terms and conditions. specific agency criteria.

Third, as is the practice of the Hong Kong PCPD regarding the status of its commissioners, in determining the status of LPPDP leaders, they can later refer to the provisions which emphasize that commissioners must be considered as civil servants, but not as government agents who receive status, immunities or privileges from the government (Personal Data Privacy) Hong Kong Ordinance, Cap. 486, Section 5(8)). With provisions like this, it reaffirms the independence of the Hong Kong PCPD which then has a big influence on the implementation of the PCPD's functions and jurisdiction so that it can reach public legal entities (government) as one of the data users freely.

Fourth, regarding the appointment, dismissal and revocation of LPPDP positions must be clearly regulated in the statutory regulations underlying its formation. The independence of an institution is also determined by the term of office of the head of the institution which must be determined with certainty (fixed) by filling positions in stages or stages (staggered), meaning that the leaders do not stop at the same time. The same thing regarding the termination of office also needs to be regulated and only determined in the regulations that form it, so that it cannot be dismissed at any time just because of the political period of the presidency.

Fifth, the LPPDP is led by the Head of the Institution and assisted by the Deputy Head who is part of the commissioners and continues to go through selection on the basis of healthy and open competition. Sixth, the President must ensure that the LPPDP has sufficient management and financial control capabilities (Zahrani, Nurmayani, & Deviani, 2022). LPPDP must have a separate public annual budget, which can be part of the overall state budget or State Revenue and Expenditure Budget (APBN). Indonesia can adopt Hong Kong PCPD practices where it has its own audit mechanism and annual report for PCPD, in this case also including the requirement to keep proper bookkeeping of all PCPD financial transactions (Personal Data Privacy) Ordinance Hong Kong, Cap. 486, Section 4 Schedule 2). It should be noted that basically the concept of independence is not without limits, because a supervisory institution must still be subject to control and monitoring mechanisms related to financial management and judicial review.

Seventh, to anticipate the ineffectiveness and lack of objectivity of institutions in providing sanctions and making decisions, there is a practice in Singapore that can be adapted in Indonesia, namely by

implementing an appeals commission. Based on Sections 48P – 48R PDPA Singapore, there is an appeal mechanism and an appeals commission (Data Protection Appeal Committee) with the task of providing opportunities for parties who have objections to PDPC decisions regarding dispute resolution (Personal Data Protection Act Singapore 2012, Section 48P- Section 48R). The establishment of this mechanism exists as a form of check and balance on PDPC decisions and to provide guarantees of legal certainty for each party.

From several recommendations and analysis considerations, the formation of a DPA carried out using a ministry based-models mechanism such as the Ministry of Communication and Information, is likely to greatly affect the independence of the institution due to the various factors described previously. In fact, the purpose of the PDP Law and the formation of implementing institutions is to ensure that all sectors, both government and private, can comply with the PDP Law, so that if you place the LPPDP under a ministry there will be a big risk of ineffective implementation of the monitoring and law enforcement functions.

3. Method

The research uses normative legal research methods with a statutory approach, a conceptual approach and a comparative approach**.**

4. Result and discussion

4.1 The Urgency of Establishing a Personal Data Protection Agency in Indonesia

Personal data protection institutions are regulated in the PDP Law, especially in Chapter IX Article 58 to Article 61. The terminology used in the PDP Law itself regarding this independent authority is the Personal Data Protection Implementing Agency (hereinafter referred to as LPPDP). Article 58 of the PDP Law states that the LPPDP is a state institution established to implement personal data protection and is responsible to the President. Regarding the LPPDP, it will be further regulated in a Presidential Regulation. LPPDP as a state institution that was born as a statutory mandate is emphasized as an institution that will be directly under the President and will be the main institution implementing the PDP Law.

LPPDP is an authority that works to prevent cyber crime, especially the misuse of personal data and information. These authorities work to secure a person's personal data at data collection centers. Data management carried out by LPPDP as an implementation of the data protection authority system (hereinafter referred to as DPA) is something that is urgent to be realized, in order to create a strong and robust cyber security system against various threats. In other words, the DPA system is a fundamental instrument in protecting personal data.

Accountability and effectiveness must be at the core of the ratification of the PDP Law to guarantee the protection of the rights of individuals or data subjects. Therefore, the existence of a regulator or authority is very necessary to be able to enforce the provisions in the PDP Law. The existence of institutions as implementers of personal data protection is also very important as a benchmark for the effectiveness of law implementation in society, considering that the elements of law according to Mochtar Kusumaatmadja are rules, principles, institutions and processes (Inggarwati, Celia, & Arthanti, 2020). According to Mochtar Kusumaatmadja, institutions as one of the pillars of law prove that their existence is very important in order to realize the application of legal principles and rules in reality or in society.

The establishment of a personal data protection authority is a manifestation of the mandate of the PDP Law to ensure the effectiveness of the principles of personal data protection and is in line with the legal definition according to Mochtar Kusumaatmadja, namely that institutions and processes are to realize the application of rules in reality. Even though the existence of a personal data protection authority is not directly stated in the constitution, this authority has constitutional importance as Article 28 G paragraph (1) of the 1945 Constitution of the Republic of Indonesia guarantees the right to privacy of its citizens.

Considering the several authorities and tasks given regarding policy formation, supervision and law enforcement carried out by the LPPDP in Articles 59 and 60 of the PDP Law, it is necessary to need a special state institution that has an autonomous nature. Institutionally, the LPPDP can no longer be categorized as a true independent state institution (independent regulatory authority), because in the aspect of formal independence the legal basis for its formation is not regulated in law but in a Presidential Regulation.

However, within the grouping of supporting state institutions, there are also known independent agencies, which are intended as government institutions that are in the executive domain and are not categorized as executive agencies or ministry/departmental institutions. Apart from that, it is important to remember that the personal data protection regulation in Indonesia itself is a comprehensive regulation, where its scope spans both the public and private sectors, therefore, to ensure the effectiveness and objectivity of the work of the implementing agency, its existence must be determined to be independent.

The independence of the LPPDP must be interpreted as two things, namely that the institution has independence over the subjects it supervises (controllers and processors of public and private data) and has independence in carrying out its duties, this means that this implementing agency may not be interfered with or controlled by other institutions/agencies including even the President. As a state institution that was born from the attribution and authority determined by the law itself, reflecting the need for an independent and comprehensive institution, the LPPDP is a non-ministerial supporting state institution that can have an element of independence that needs to be guaranteed by the commitment of the President and future commissioners. Even though in formal terms the LPPDP is not an independent state institution because the legal basis for its formation is not based on higher laws and regulations, it does not rule out the possibility for an institution to become an independent agency which has an element of independence in several aspects of carrying out its duties and institutional resistance. state when exercising its authority (karo-karo, 2019).

The existence of an independent DPA in several international legal instruments is also stated as a condition for fulfilling minimum standards in protecting personal data. Regarding the exercise of power and authority of supervisory authorities in each country, it varies depending on the legal system and constitutional system adopted. The independence of the DPA is an important indicator that determines the legal adequacy of personal data protection in Indonesia with other countries, especially when compared to developed countries in the European Union which enforce the EU GDPR. Achieving this adequacy will not only make it easier to regulate data transfers and cross borders, it will also encourage the stability of the digital economy in Indonesia (Trilestari & Suriaatmadja, 2021).

The independence referred to is that in carrying out its duties and functions, the DPA is free from internal and external influence, political and economic influence. According to the EU GDPR, independence is also an essential element to ensure effective protection of individual rights and freedoms in terms of the processing of individuals' personal data. Because personal data processing is increasingly complex, a personal data protection supervisory authority must be established as a supervisory institution that is free from all intervention from both public and private bodies as processors and controllers of public data.

The provisions contained in the EU GDPR do not only apply to processors and data controllers operating in Europe, but also apply to all providers of services or goods that monitor the behavior of individuals located in Europe. The provisions of Article 52 EU GDPR regarding independence requirements are the benchmark for the formation of DPAs in European countries so that they can be qualified as independent supervisory authorities who act as supervisors and law enforcers who meet adequacy. The indicators of independence emphasized in Article 52 EU GDPR include:

1) Institutional independence, meaning that each supervisory authority must act with complete independence in carrying out its duties and exercising its powers in accordance with the law. Institutional independence must be guaranteed in the legal basis for its formation, this is because the statutory regulations that underlie the formation of the institution will have implications for the

process of selecting, appointing and dismissing commissioners, where this process must be able to obtain commissioners who have integrity, capability and strong acceptability. in public.

2) Commissioner independence, the supervisory authority must be free from external influence, both directly and indirectly, and is not permitted to receive instructions from anyone. Ensuring the independence of commissioners needs to be carried out from the time of their appointment or appointment through transparent procedures at least by parliament, government, head of state, or by an independent body entrusted based on the laws and regulations of each country (European Union General Personal Data Regulation, Regulation 2016/ 679, Article 53).
3) Organizational independence, meaning that the state must support the supervisory authority by providing the necessary resources and infrastructure, technical and financial capabilities so that it can carry out its duties effectively. Organizational independence is related to institutional independence, as well as having autonomy to determine technical regulations such as system structuring, internal supervision, personnel and financial supervision.
4) Independence of human resources, the state must ensure that each supervisory authority selects its own staff, selected by the supervisory authority or an independent body established by law, and subject to the direction of the commissioner or member of the supervisory authority concerned. Through the independence of human resources, the DPA has the opportunity to form its own staffing model, at least commissioners must have qualifications, experience and skills, especially in the field of personal data protection, which are necessary to carry out their duties and authority (European Union General Personal Data Regulation, Regulation 2016/679 , Article 53(b)).
5) Financial control, the DPA must have financial controls that do not affect its independence and have a separate public annual budget, which can be part of the overall state budget (APBN). An independent supervisory authority must have the autonomy to control its own finances without reducing state audit mechanisms, monitoring related to financial management, and judicial review.

In practice, the provisions of Article 52 EU GDPR provide flexibility for countries in Europe to form one or more of their own DPAs with a model left to each country. This is because this provision itself does not rigidly regulate the form or model of DPA which is categorized as an independent supervisory authority. However, the relaxation provided by Article 52 EU GDPR does not rule out its essence as a general standard of DPA independence in European countries and every member is obliged to comply with this provision. In several countries in the EU that do not adhere to the single supervisory authority model, DPAs are attached to existing institutions by adding authority to these authorities and still complying with the minimum standards of independence in Article 52 EU GDPR.

Even though in the constitutional context of the European Union, the DPA was not formed using a single supervisory authority model, in the sense that the DPA is under the government or executive, as long as the DPA is stipulated in the laws and regulations that created it as an independent state institution and can play its function as a supervisory authority that meets the requirements and the qualifications in Article 52 EU GDPR, then the DPA can be said to be an independent institution. In the EU GDPR, there are several main keys to ensuring that personal data protection in a country is effective (Daesyifa Bunga Hartawan, Tri Andrisman, Budi Rizki Husin, 2024). First, a DPA must be established and stipulated in national law. Second, the DPA must be able to act with full independence in accordance with the minimum standards of independence set out in Article 52 EU GDPR which is then guaranteed by the personal data protection law in the country itself. Third, the independent nature of the supervisory authority is reflected in its organizational structure and commissioners.

Basically, the concept of independent institutions in developed countries and developing countries has different political systems. The formation of the DPA as an independent state institution must of course pay attention to the state's readiness starting from the basic regulations that form it, the selection process for state institutions, protocol rights, institutional financing, employment status, to legal political direction. The independent characteristics as regulated in the EU GDPR need to be implemented because in the future the LPPDP will not be an assistant to the government, but rather a supervisory institution that can carry out its functions and authority over all data controllers and processors from public and private bodies to guarantee human rights in the realm of privacy.

In Indonesia, one of the independent state institutions that can be used as reference material in the formation of the LPPDP as a supervisory authority that has independence is the Business Competition Supervisory Commission (KPPU). Institutionally, the KPPU is an independent, non-structural institution that is independent from the influence and power of the government and other parties, and is responsible to the President. KPPU was formed as an implementation of Law Number 5 of 1999 (Business Competition Law) and has explicitly stated the independence of KPPU. In the context of the KPPU, although it is responsible to the President, institutionally the KPPU is an independent state institution in carrying out its functions and authority as a business competition supervisory institution. From the provisions on appointment, dismissal and funding, it can be seen that in the formal aspect, the provisions characterize the characteristics of independent state institutions. The mechanism for appointing and dismissing KPPU commissioners is carried out by the President with the approval of the DPR.

With an approval and confirmation process mechanism with the DPR, the President will be more careful in appointing and dismissing prospective commissioners. Apart from that, with this mechanism the public can be involved and control the confirmation process carried out by the DPR. By ensuring that LPPDP is an independent institution in carrying out its duties, Indonesia can actively participate in cooperation in enforcing the protection of personal data in the international scope, the interests of data transfer and cross-border, participate in the formation of international standards and is important for attracting foreign investment. Indonesia (Malik, 2013).

The regulations establishing the LPPDP need to firmly and clearly formulate the independent nature of the LPPDP, so that in carrying out its functions and authority the LPPDP is free from intervention and interests of any individual, political or institutional entity. The scope of the PDP Law which does not separate its application to just one sector, where data controllers and processors from public and private bodies are obliged to comply with the same rules is a clear basis for why the LPPDP needs to have independence. Because of the supervisory and investigative authority vested in the LPPDP, the LPPDP must be able to assert its independence as a non-structural institution that is free from political pressure, the influence of interests and the power of any institution/agency, and is responsible to the President (Tejomurti, Hadi, Imanullah, & Indriyani, 2018).

4.2 Opportunities and Challenges for Establishing a Personal Data Protection Agency in Indonesia

The formation of LPPDP is an innovation in data management or what is known as Big Data. In fact, the formation of the LPPDP must be realized immediately in Indonesia, bearing in mind that the presence of this authority is in line with the government's mission to carry out sustainable development (sustainable development goals), especially goal 9, namely industry, innovation and infrastructure. This authority provides guarantees regarding the security of internet users' data, this is based on the fact that the authority works through an integrated system with Kominfo, which is responsible for managing internet users' data (Latumahina, 2014).

The absence of a specific personal data protection authority in Indonesia has implications for investors and companies' distrust in terms of "data storage." Furthermore, if there is an independent institution or body that supervises the data protection authority (hereinafter referred to as DPA) it can have a positive impact such as an economic perspective which ultimately supports Indonesia as a business and investment center as well as global data management and a trusted and extensive data management industry. in terms of data storage such as cloud computing which can develop in Indonesia (Medlimo, 2022). Apart from the institutional formation of the LPPDP, a supervisory authority must of course be equipped with comprehensive authorities so that it can carry out its functions and duties effectively. In Article 60 of the PDP Law, authority has been determined which can be described and compared with the authority of the Hong Kong PCPD and Singapore PDPC as follows:

1) LPPDP has the authority to form policies in the field of personal data protection. This authority shows that the LPPDP as a regulator is needed for can establish and formulate pragmatic and technical rules not yet in the PDP Law. This authority also belongs to the Hong Kong PCPD which based on PDPO is empowered to establish codes of practice;

2) LPPDP has the authority to supervise controller compliance personal data. Basically this is the main function of formation each DPA, namely as an institution that monitors, monitors, and monitor the compliance of each person and sector with the provisions of the PDP Law;
3) LPPDP has the authority to carry out cooperation and coordination with DPA other countries, law enforcement officials and other state institutions involved in framework for protecting personal data. Same with PCPD Hong Kong and PDPC Singapore, both have the authority to enter into cooperation with international bodies to develop privacy protections and personal data by carrying out promotions, activities, services, or create an MoU between countries that has legal equality laws and DPA (Alim, Triono, & Yudhi, 2023).
4) LPPDP has the authority to receive complaints and/or reports of allegations violation of personal data protection. One of the essence of data protection privacy is the guarantee of the data subject's right to protect data personally, namely by submitting a complaint or report to the appropriate authority authorized. In Hong Kong PCPD practice, it is not just accepting filing a complaint, PCPD also provides legal assistance to the subject data to formulate the complaint so that it can be processed. PCPD Hong Kong provide legal assistance and usually the PCPD will cover the costs law in providing legal assistance to the reporter (Privacy Commissioner for Personal Data). Apart from that, Hong Kong PCPD too provides lawyer services (duty lawyer service) through Seknal Tel-Law which is an automated answering service that provides legal information that recorded free of charge by telephone and available in Cantonese, Putonghua, and England. Meanwhile in Singapore, PDPC does not provide it legal advice or legal advice for the community. However, PDPC provides a question and answer feature that can respond automatically on the official website (Yolanda & Hutabarat, 2023).
5) LPPDP has investigative and inspection authority. Basically Investigative authority is one of the basic authorities that must exist to a supervisory authority for personal data protection so that it can be realized ideals and objectives of the law. As is the practice in several countries which already has its own DPA, investigations and inspections become authority that must exist in order to carry out law enforcement functions effectively;
6) LPPDP has the authority to carry out law enforcement actions and impose penalties administrative sanctions. In addition to carrying out supervisory duties and The regulator also plays a role in deciding administrative fines. Likewise with PCPD Hong Kong, through PDPO as policy has comprehensively determined the sanctions that can be imposed by the PCPD to violators. PDPC Singapore also has the same authority namely being able to impose sanctions on violators and decisions PDPC can appeal to the Appeals Commission based on the provisions PDPA;
7) LPPDP has corrective authority and issues orders/direction as a follow-up to the results of supervision. Authority to provide direction and Improvement as a follow-up to the results of supervision is important before the law enforcement process continues. Authority to create Improvement decisions, directions, and enforcement notices are also owned by PCPD Hong Kong and PDPC Singapore, each of which is regulated by procedures implementation in PDPO and PDPA;
8) LPPDP is given the authority to facilitate external dispute resolution non-litigation court/adjudication. By being given facilitation authority settlement of disputes outside of court, it is necessary to pay attention formation of the institution into an institution that should have authority sufficient to face and carry out their duties and functions. If the supervisory authority believes that the complaint or report received can use alternative dispute resolution processes, then as is practice in PCPD Hong Kong and PDPC Singapore this can be done using a scheme settlement through conciliation or mediation first.

The institutional model and authority of countries that already have DPAs will depend greatly on their respective legal systems and constitutional systems. It is hoped that this comparative research regarding personal data protection supervisory authorities in Hong Kong and Singapore can provide material for consideration and study in determining the appropriate and ideal model for the LPPDP. Thus, the process of establishing the LPPDP must be of serious concern to all parties, especially stakeholders. Without sincere and pure intentions from the authorities, the process of establishing a data protection authority system will only be static, therefore every policy should be prepared systematically in order to save and normalize national life in accordance with the demands of reform, in this case with the formation of the LPPDP in Indonesia.

Based on the criteria that have been explained, the direction for establishing LPPDP as a data security authority must have a framework that is prepared systematically, coherently and coherently. In this effort, it is hoped that the formation of the LPPDP will not be a bubble or temporary, but will become a foundation that guarantees people's security and comfort when using the internet.

5. Conclusion

The urgency of establishing LPPDP in Indonesia is to provide legal certainty regarding the protection of people's personal data. Therefore, it is necessary to have an independent personal data protection supervisory authority. Independence emphasizes that the LPPDP must be independent, and free from intervention and interests of individuals, politics or any institution in making decisions, carrying out its functions, duties and authority as regulated in the PDP Law and its implementing regulations, including being free from the political will of the President as the holder supreme executive power.

Institutionally, the LPPDP has been mandated to be an institution in the executive branch, however, independence must be attached to the LPPDP as a minimum standard and considered as a need for strong authorization. Practices and developments in Hong Kong and Singapore can be an example in studying different institutions in forming personal data protection supervisory authorities in Indonesia
The formation of LPPDP in Indonesia faces several challenges. First, relating to the institutional model, whether to form the LPPDP with a single independent supervisory authority model that is directly responsible to the President like the Hong Kong PCPD or to form the LPPDP by implementing a ministry-based model, meaning that the supervisory authority is formed and is responsible to the President through the relevant Minister like the Singapore PDPC practice. The next challenge is related to the limits of authority so that there is no overlap between one institution and another, so in-depth analytical studies are needed in order to create an institution that is independent and has independence.

References

Akib, M., Triono, A., Tisnanta, H., & Medlimo, R. A. (2023). Application of strict liability principles in environmental dispute resolution. *Annals of Justice and Humanity*, *2*(2), 65-75.

Alim, M. Z. (2023). The role of waste banks in realizing good environmental governance in Bandarlampung City. *Journal of Governance and Accountability Studies, 3*(1), 51-61.

Alim, M. Z., Triono, A., & Yudhi, R. (2023). The right to environmental cleanliness through waste management in West Lampung Regency. *Annals of Justice and Humanity, 2*(2), 53-63.

Arafat, Y. (2015). Prinsip-prinsip Perlindungan Hukum yang seimbang dalam kontrak. *Jurnal Rechtens, 4*(2), 25-39.

Aurora, S. D., Tisnanta, H., & Triono, A. (2023). Right to health services for people with HIV/AIDS in Bandarlampung: Challenges and fulfillment. *Annals of Justice and Humanity, 2*(2), 77-87.

Hakim, J. (2019). Exoneration Clause on Law of Consumer Protection: Effects and Legal Efforts. *Jurnal Hukum Dan Peradilan, 8*(2), 297-314.

Inggarwati, M. P., Celia, O., & Arthanti, B. D. (2020). Online Single Submission For Cyber Defense and Security in Indonesia.

karo-karo, R. (2019). Penegakan hukum kejahatan dunia maya (Cyber crime)

Kartika, A. D., & Medlimo, R. A. (2023). Development Taman Surya Nusantara to increase new and renewable energy in Indonesia. *Journal of Sustainable Tourism and Entrepreneurship, 4*(3), 319-330.

Kartika, A. D., Septiana, D., Ariani, N. D., Kasmawati, K., & Nurhasanah, S. (2022). Implementation of Prudential Principles in Providing Credit Loans to Shopee Marketplace Consumers. *Studies in Economy and Public Policy, 1*(1), 27-38.

Khan, M. M. R., & Sultana, R. (2021). Shift in the role of criminology in criminal law: Reflecting the doctrinal change. *Annals of Justice and Humanity, 1*(1), 1-10.

Latumahina, R. E. (2014). Aspek Hukum Perlindungan Data Pribadi di Dunia Maya.

Malik, P. (2013). Governing big data: principles and practices. *IBM Journal of Research and Development, 57*(3/4), 1: 1-1: 13.

Medlimo, R. A. (2022). Inovasi Pemberdayaan Industri Kreatif Nasional Sebagai Upaya Pemulihan Perekonomian Nasional Ditinjau Berdasarkan Konsep Pentahelix. *Maliyah: Jurnal Hukum Bisnis Islam, 12*(2), 56-72.

Medlimo, R. A. (2024). Penerapan Prinsip Strict Liability Dalam Penyelesaian Sengketa Lingkungan Hidup.

Rahma, S., Triono, A., & AT, M. E. P. (2023). Implementing social security programs for employees in Bandar Lampung: Challenges and recommendations. *Journal of Governance and Accountability Studies*, *3*(2), 109-119.

Sudaryanti, K. D., Darmawan, N. K. S., & Purwanti, N. P. (2013). Perlindungan Hukum Terhadap Investor Dalam Perdagangan Obligasi Secara Elektronik. *Kertha Wicara, 2*(1), 1-5.

Tejomurti, K., Hadi, H., Imanullah, M. N., & Indriyani, R. (2018). Legal Protection for Urban Online-Transportation-Users' Personal Data Disclosure in the Age of Digital Technology. *Padjadjaran Jurnal Ilmu Hukum (Journal of Law), 5*(3), 485-505.

Trilestari, S. I., & Suriaatmadja, T. T. (2021). Tanggung Jawab Penyelenggara Platform Jual Beli Online Terhadap Kebocoran Data Pribadi Pengguna Berdasarkan Peraturan Tentang Informasi dan Transaksi Elektronik Dihubungkan dengan Pasal 1366 Kuhperdata Tentang Tanggung Jawab Berdasarkan Kelalaian. *Prosiding Ilmu Hukum, 7*(1), 153-157.

Yolanda, E., & Hutabarat, R. R. (2023). Urgensi Lembaga Pelindungan Data Pribadi Di Indonesia Berdasarkan Asas Hukum Responsif. *Journal of Syntax Literate, 8*(6).

Zahrani, S. S., Nurmayani, N., & Deviani, E. (2022). Preventing early marriage in North Lampung Regency: An analysis of the efforts of the Ministry of Religion's Office. *Dynamics of Politics and Democracy, 2*(1), 23-35.