



PROTECTION OF INDONESIA'S PERSONAL DATA AFTER THE RATIFICATION OF THE DRAFT PERSONAL DATA PROTECTION LAW

Siti Yuniarti ¹

Business Law Program, Faculty of Humanities, Bina Nusantara University,
Email : yuniarti@binus.ac.id

Abstract: *The protection of Indonesia's personal data entered a new chapter with the signing of the Personal Data Protection Law by the President on October 17, 2022. The presence of the Personal Data Protection Law (PDP Act) is a lex specialist of Indonesian personal data protection regulations. This study analyzes how the protection of Indonesian personal data after the enactment of the PDP Act by using components in the personal data protection ecosystem as parameters, namely data subjects, data controllers and data processors, data protection officers and supervisory agencies protection of personal data. Using normative legal research methods, this study found that the regulation of the 4 (four) components has been accommodated in principle in the PDP Act. The balance between the protection of individuals on the one hand and the public interest on the other is tried to be accommodated in the principles behind the PDP Act and the reduction of the implementation of some norms. The composition of the norms shows that the processing of personal data, especially the obligations of the data controller, is the focus of regulation. The role of a data protection officer to ensure regulatory compliance is complemented by a risk mitigation function. The existence of data protection as service is also accommodated in the PDP Act. The supervisory institution is given a series of authorities with details of investigative authority. The PDP Act as a compact regulation requires various implementing regulations, including provisions issued by institutions and sectoral regulations. The support of understanding and strengthening of all parties in the personal data protection ecosystem absolutely needs to be carried out immediately as an effort to realize compliance by minimizing the failure of protection and unauthorized processing as a preventive measure. Preventive measures should be used as a key option in the data protection regime. Therefore, discussions regarding the protection of personal data continue to move dynamically following emerging legal and social developments.*

Keywords: *Privacy, Personal Data Protection, Indonesia.*

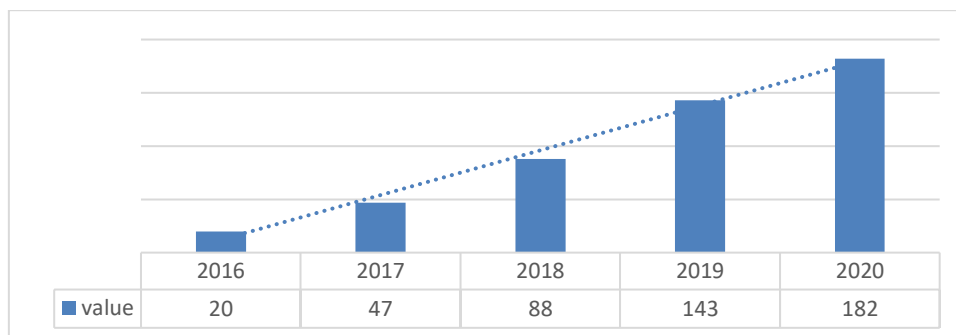
I. INTRODUCTION

Indonesia's personal data protection regime is entering a new chapter. The long journey of drafting legislation on the PDP Act was initiated with the preparation of an Academic Manuscript in 2014 (Dirjen IKP, 2014). The PDP Bill was proposed by

the Government to be discussed with the DPR since December 2021 and reached the final point with the passage of the PDP Bill at the Plenary Meeting of the DPR on September 20, 2022 and signed by the President on October 17, 2022. Furthermore, Indonesia became the 5th country in ASEAN to have special regulations for personal data protection after Singapore, Malaysia, the Philippines, Thailand and Laos.

The long journey of discussion of the PDP Bill until the ratification process by the DPR was marked by a deadlock on the institutional form of the personal data protection supervisory authority or data protection agency (Burhan, 2021). Various urges arose for the House of Representatives and the Government to immediately complete the discussion of the PDP Bill as conveyed by the *Koalisi Perlindungan Data Pribadi*. The discussion process was also marked by the news of a series of incidents of failure to protect personal data, both experienced by public and private Electronic System Operators (PSE) (Data Pribadi, 2018)). Reports received by *Polisi Siber* showed an increase in cases of data theft during the period 2016-2020. Therefore, the passage of the PDP Bill is considered a step forward to provide protection to the people. (BBCNews, 2022)

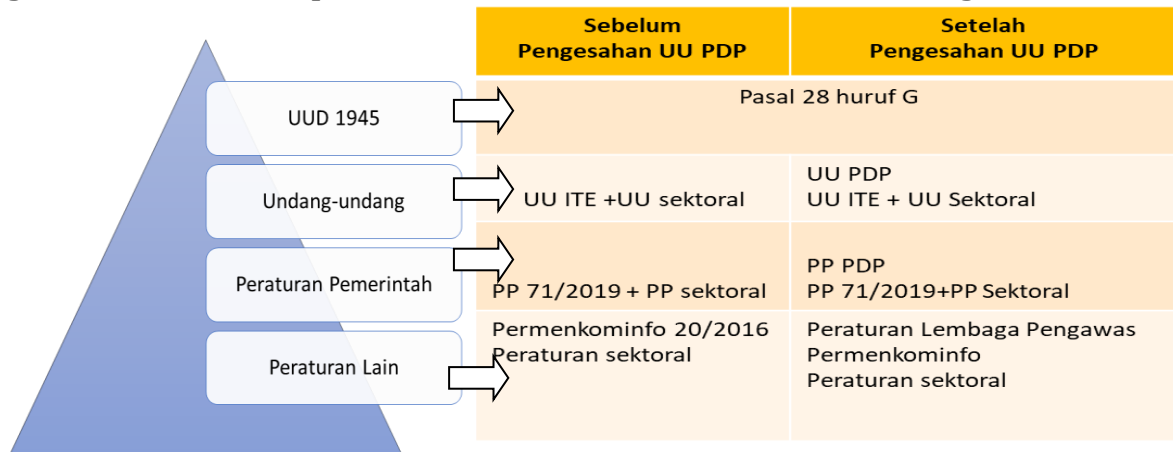
Figure 1 Personal Data Protection Failure Case (Jayani, 2021)



In terms of legislation, the issue of personal data protection has been mentioned in approximately 30 (thirty) regulations in Indonesia, but has not specifically regulated the protection of personal data (ELSAM, 2016). The ratification of Act No.11 of 2008 on Electronic Information and Transactions as amended by Act No.19 of 2016 ("ITE Act") is a step forward in regulating the protection of personal data. However, the ITE Act only provides for the approval of data subject in the processing of personal data, the filing of claims for compensation and the deletion of irrelevant information. The legal vacuum is bridged with the implementing regulations of the ITE Act, namely Government Regulation No. 80 of 2012 concerning the Implementation of Electronic Systems and Transactions which was further amended by Government Regulation No. 71 of 2019 ("PP 71/2019") as well as regulations at the ministry level. Together with the ITE Act and implementing regulations, sectoral regulations are issued to regulate the protection of personal data such as regulations issued by Bank Indonesia, the Financial Services Authority, the Ministry of Trade. The presence of the PDP Act become a *lex specialist* for the regulation of personal data legal protection in Indonesia (M.Ramli, 2022) .

Therefore, the current legislation on the protection of personal data in Indonesia can be illustrated in the figure below.

Figure 2 Map of Indonesia's Personal Data Protection Legislation



Source: Author, 2022.

The enactment of the PDP Act as a *lex specialist* in personal data protection regulation has the consequence of understanding the regulations in it as a first step in understanding the protection of Indonesian personal data. Therefore, this study then discusses how Indonesia's personal data protection arrangements in the PDP Act under components in the personal data protection ecosystem as parameters, namely data subjects, data controllers and data processors, data protection officers and personal data protection supervisory agencies. Of course, this writing is an initial writing that will continue to develop in line with the development of the implementing regulation of the PDP Act as well as the rules issued by personal data protection supervisory agencies and sectoral arrangements. It is hoped that through this study, a preliminary overview of how the current regulation of personal data in Indonesia is obtained which is useful for data subjects and every individual and institution that processes the personal data of Indonesian citizens and / or carries out processing activities in the territory of Indonesia.

This research uses normative legal research methods that focus on values, norms and written rules. As normative legal research, this research is carried out through laws and regulations and literature studies which are classified as secondary data. Then, the research approach used is a statutory approach that focuses on regulations related to the research topic, namely the PDP Act.

II. DISCUSSION

The personal data protection regime basically seeks to ensure that the process of collecting, processing, storing and deleting/destroying data by data controllers and data processors is carried out by applying the principles of personal data protection and putting the rights of data subjects as the main thing. Other component is a data protection officer as a function that ensures the compliance of data controllers and / or data processors to personal data protection regulations and the existence of a

personal data protection supervisory agency as an institution which has the function of constituting policies and supervision of personal data protection is another component that appears in the personal data protection ecosystem. The PDP Act consists of 16 Chapters and 76 articles in terms of regulatory structure that accommodates the four components of the personal data protection ecosystem. Referring to the percentage of regulation, the emphasis of the PDP Act regulation is on the processing of personal data, in particular the obligations of the personal data controller as described in the table below.

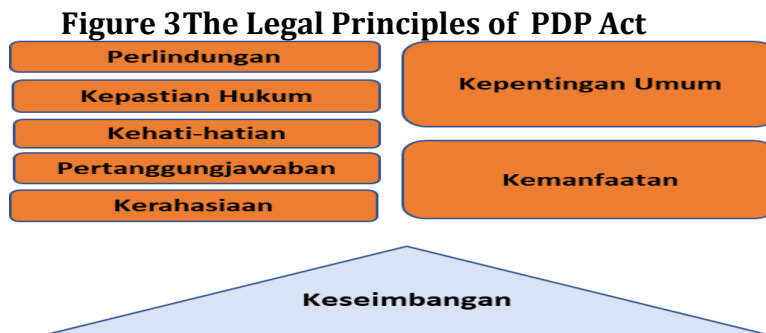
Table 1 Composition of the PDP Act

No.	Subject	Number of Articles	Percentage
1	General provisions	2	2,6%
2	Principles	1	1,3%
3	Types of personal data	1	1,3%
4	Rights of personal data subjects	11	14,5%
5	Processing of personal data	3	3,9%
6	Obligations data controller and data processor on data processing	36	47,4%
	a. General (1)		
	b. Obligations of data controller (31)		
	c. Liability of data processor (2)		
	d. Officials or officers who carry out data protection function (2)		
7	Transfer of Personal Data	2	2,6%
	a. On Indonesia jurisdiction (1)		
	b. Outside Indonesia jurisdiction (1)		
8	Administrative sanctions	1	1,3%
9	Institutional	4	5,3%
10	Cooperation international	1	1,3%
11	Participation of the community	1	1,3%
12	Dispute Settlement and procedural law	1	1,3%
13	Prohibition on data protection utilisation	2	2,6%
14	Criminal provision	7	9,2%
15	Transitional terms and closing provisions	3	3,9%
	TOTAL	76	100%

Source: Author, 2022.

The protection of personal data in the PDP Act is a manifestation of the protection of the human rights of citizens as stated in Article 28G paragraph (1) of the UUD 1945. Restrictions on the exercise of human rights in the name of the public interest seek to be balanced through the principles underlying the PDP Act as illustrated in the Figure below. Balance principle is an affirmation of the PDP Act's efforts to balance the two components. Explanatory of PDP Act as an official interpretation states that the PDP Act is basically a general standard and is open for each sector to implement personal data protection according to the characteristics of each sector.

This has been done previously by Bank Indonesia and the Financial Services Authority in the context of consumer protection and the Ministry of Trade in the context of electronic system-based trade or e-commerce.



Source: Author, 2022.

The scope of the applicability of the PDP Law is extra-territorial by referring to the location of activities and the consequences of such activities as long as they are related to the territory of Indonesia and/or Indonesian citizens. Global personal data protection legislation has 2 (two) patterns related to the scope of regulatory subjects. First, processing by public institutions as part of legislation as used by China. Second, data protection legislation only applies to the processing of personal data by private institutions such as Singapore. In this regard, the PDP Act refers to the first pattern in which the subjects of legislative regulation are public bodies, private (persons and corporations) and international organizations. An exception to the applicability is given to the processing of personal data by an individual person in a personal or household activity. It should be underlined that the classification of public bodies in the PDP Act is to include bodies that obtain public and/or foreign donations. This is in line with the definition of Public Bodies in the Public Information Disclosure Act. The consequence of such arrangements is that the obligations and responsibilities of data processing apply to both public and private institutions. The variety of actors processing personal data in the private sphere has a wide scope, ranging from private individuals, MSMEs to global corporations. Therefore, it is necessary to make efforts to encourage the readiness of various layers of data processors both in terms of understanding, infrastructure and technical arrangements by taking into account their respective characteristics.

Object of the PDP Act is personal data itself. The terminology of personal data is defined as "data of an individual identified or identifiable individually or in combination with other information either directly or indirectly through electronic or non-electronic systems". This definition is in line with the definition of personal data in other regulations such as PP 71/2019. Thus, the scope of personal data referred to in the PDP Law is data attached to human individuals (*natuurlijk persoon*) and does not include corporations. Personal data is then classified into 2 (two) groups using the component "consequences of data processing on data subjects" as parameters, namely personal data of a general nature and personal data of a sensitive nature. The types of general personal data are limited to the scope of the data described in Article 4 (3) of the PDP Act, but allow variations that arise from

the combined personal data. In contrast, sensitive types of personal data are still open for addition as long as they are in accordance with laws and regulations. The difference in data classification has consequences when processing data that is the obligation to conduct prior assesment impact of processing by the personal data controller if the semsitive data shall to be processed.

Figure 4 Classification of Personal Data - PDP Act



Source: Author, 2022.

1. Data Subjects

The focus of personal data protection is data subjects. The data subject's control over matters relating to himself is given through an approval mechanism. Strengthening the protection of data subjects is also carried out by providing data subjects with a series of rights related to the processing of their personal data. The rights of data subjects stipulated in each personal data protection regulation are varied. The PDP Act itself provides 9 (nine) rights for data subjects as described in the Table below. The right for data subjects on the one hand and on the other hand gives rise to the obligation of fulfillment by the data controller with the time limit specified in the PDP Act. In addition to the time limit for fulfillment, it should also be necessary to regulate the obligation for the data controller to provide methods or tools that assist data subjects to exercise their rights easily, simply and efficiently. The easiest examples are the immediate visible placement, the use of simple terminology and language for privacy policy as an implementation of the right to information. However, the exercise of the 9 (nine) rights of the data subjects does not apply to matters classified as related to the public interest as stipulated in Article 15 of the PDP Act or endangering the data subject or others and/or impacting the personal data of others as described in the Table below. Thus, the rights of data subjects that cannot be reduced in the PDP Law only include 3 (three) types of rights, namely: (a) the right to information; (b) the right to complete, renew, correct errors or inaccuracies; and (c) the right to indemnity.

Table 5 Right of Data Subject – PDP Act

Data Subject Rights	Deadline Fulfillment	Exception (Basis: Public Interest- Psl 15 PDP Act)
1 Right to information	X	X
2 The right to complete, update, correct errors and/or irregularities	3x24 hours	X
3 Right of access	3x24 hours	Available*
4 Right to terminate processing, erasure, destruction	X	Available
5 Right to withdraw consent	3x 24 hours	Available
6 Objection right to automated processing	3 x24 hours	Available
7 Right to delay/restrict processing	X	Available
8 Right to indemnity	X	X
9 Right of use of personal data by data subjects or other personal data controllers	X	Available

*In addition to restrictions in the public interest, restrictions if they cause harm/physical/mental harm to the data subject or others and/or have an impact on the personal data of others.

Source: Author, 2022.

The right of data subjects to request erasure is a part of data subjects' rights regulated in the ITE Act and the PDP Act. In the ITE Act, data subjects are given the right for delete of irrelevant information's request to the PSE or are often interpreted as a right to be forgotten. The mechanism used is through a court determination. PP 71/2019 as the implementing regulation of the ITE Act further translates the provisions regarding the deletion of irrelevant information as a PSE obligation (right to erasure) as requesting to PSE and expenditures from search engine data (right to delisting) carried out through court mechanisms. The PDP Act distinguishes between the activities of erasure and destruction of personal data. Destruction of personal data refers to the explanation of Article 44 of the PDP Act covering the eliminating, obliterating or destroying personal data with the aim that personal data can no longer identify data subjects. The erasure and destruction activities in PP 71/2019 and the PDP Act have the same purpose, namely no longer accessible personal data, but the basis of the actions underlying the implementation of the deletion and/or destruction activities is different as outlined in the Table below

Table 6 Legal Basis of Data Protection Erasure

	Right to Erasure PP 71/2019	Erasure PDP Act	Destruction PDP Act
Processing without the consent of the data subject	v		
Withdrawal of consent by data subjects	v	v	
Unlawful acquisition and processing	v	v	v
No longer needed to achieve processing purposes	v	v	
Expiration of usage time limits and/or retention periods	v		v
Causing harm to data subjects	v		
Data subject requests		v	v
Not relating to the legal process of a case			v

Source: Author, 2022.

2. Data Controller and Data Processor

Discussions about data controller components and data processors cannot be separated from the data processing activities themselves. Explicit valid consent is a valid legal basis for the data controller to carry out data processing and is carried out by applying the principles of personal data protection, in addition to the conditions that allow the processing of personal data as stipulated in Article 20 paragraph (2) (b)-(f) of the PDP Act. Referring to the principles of personal data protection in the Privacy Framework published by the Organization for Economic Co-Operation and Development (OECD) (OECD, 2013), the PDP Act has reflected that principles.

Table 7 OECD Personal Data Protection Principles-PDP Act

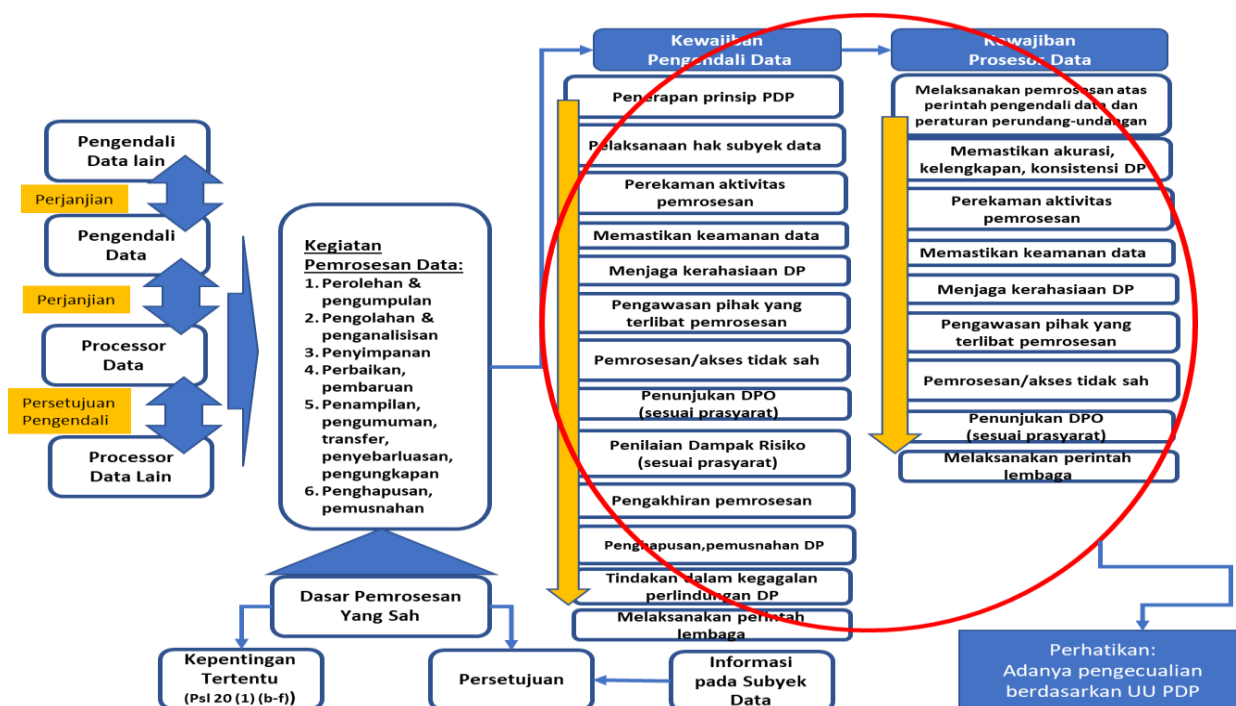
OECD	PDP Act
Collection limitation principles	The collection of Personal Data is limited and specific, legally valid, and transparent
Data Quality Principles	The processing of Personal Data is carried out accurately, completely, not misleadingly, up-to-date, and accountable
Purpose specification principles	The processing of Personal Data is carried out by notifying the purposes and activities of the processing, as well as the failure of the Personal Data Protection
Use limitation principles	<ol style="list-style-type: none"> a. The processing of Personal Data is carried out in accordance with its purposes; b. Personal data is destroyed and/or deleted after the retention period expires or at the request of

	the personal data subject, unless otherwise provided by laws and regulations.
Security safeguard principles	The processing of Personal Data is carried out by protecting the security of Personal Data from unauthorized access, unauthorized disclosure, unauthorized alteration, misuse, destruction, and/or disappearance of Personal Data
Individual Participation principles	The processing of Personal Data is carried out by guaranteeing the rights of the Personal Data Subject
Accountability principles	The processing of Personal Data is carried out responsibly and can be clearly proven.

Source: Author, 2022.

Obligations of data controllers and data processor on data processing activities is the most regulated in the PDP Law. In addition to the consent and application of personal data protection principles, data controllers and data processors are also given obligations and responsibilities as described in figure below. Data processing of children and persons with disabilities is also the scope of data processing arrangements.

Figure 5 Data Controller and Data Processor Obligations - PDP Act



Source: Author, 2022.

The processing of personal data may be carried out by the data controller himself or another party referred to as the personal data processor with an agreement as the basis of the legal relationship. The responsibility of data processing, even though it is carried out by the personal data processor, remains with the data controller. This essentially provides legal certainty for data subjects regarding liability in the processing of their personal data. Therefore, there are two provisions in the PDP Act that at least need to be re-discussed or at least given detailed arrangements in this regard. First, the provisions regarding the limitation of the responsibility of the data controller in terms of the actions of the data processor outside the commands and purposes set by the data controller. Second, regarding the appointment of another party as a personal data processor by the initial personal data processor based on the consent of the personal data controller. The impact of both arrangements will be related to the legal relationship between the data subject and the party carrying out the processing of his personal data including in the event of a dispute.

An issue that often arises in personal data protection regimes is the failure to protect personal data. In the event of a failure to protect personal data, the PDP Act requires notification to data subjects and institutions. Under certain conditions, information is provided to society. Knowledge of data subjects may be excluded in the event of conditions related to national defense and security, law enforcement, state administration and supervision of the financial services sector, monetary, payment system and financial system stability as stated in Article 50 of the PDP Act. Of course, in technical regulations, data protection failures are followed by technical activities as PP No.71/2019 regulates interference with electronic systems.

3. Data Protection Officer

The PDP Act uses the terminology of an Officer who carries out a personal data protection function (hereinafter referred to as an "Officer") to describe the function/position of the data protection officer. The function of the Officer is to ensure compliance with the principles of personal data protection and mitigation of personal data protection risks. In the Grand Design of DPO Indonesia, it is stated that the terminology of a data protection officer is different from the scope of the Officer who carries out the personal data protection function in the PDP Act. The difference refers to the difference in the main function, namely the duties of a data protection officer are defined as an internal consultant who ensures that the personal data protection function is carried out in his organization with the duties carried out by occupations of different positions. Meanwhile, the Officers who carry out personal data protection functions which include legal and compliance, governance, management and technical functions. (Komunikasi, 2021)

The existence of officers in the data control organization is not an obligation as long as the data controller and data processor are not meet the qualifications to appoint officers as stated in the PDP Act. The appointment of an Officer shall be made in the event of: (a) processing in the term of public service; (b) core activities have a nature, scope and/or purpose that require regular and systematic monitoring of personal data on a large scale; and (c) core activities consist of large-scale

processing of data for personal data of a specific nature and/or relating to criminal acts.

The qualification of the appointment of Officers in the PDP Act certainly requires further reprieve, considering that some qualifications require certain benchmarks such as "core activity", "large-scale" qualifications. It also conduct by personal data protection legislation that uses these qualifications. For example, the provisions of the 2017 Guidelines on Data Protection Officers (DPOs) in the implementation of GDPR where it is stated that "core activities" refer to key operations necessary to achieve the purpose of data processing by data controllers or data processors. For example, the core activity of the hospital is to provide health services. These health benefits cannot be provided safely and effectively without processing health data. Therefore, processing data should be considered a core activity of the hospital. (Party, 2017).The "large-scale" issue proposed in the 2017 Guidelines on Data Protection Officers (DPOs) refers to certain components as a benchmark in the form of the number of data subjects, data volume, duration of activity and geographic reach of data processing.

The roles and functions of officers in the PDP Act include the functions of: (a) providing information and advice; (b) monitor and ensure compliance; (c) provide advice on impact assessments and ensure their implementation; and (d) as a contact person. The four functions when classified can be sorted into compliance functions which include the functions in letters (a) and (b) above, the risk analysis function and the contact person function as described in figure below.

Figure 6 Functions of Officer - PDP Act



Source: Author, 2022.

In addition to the preparation of officer competencies to support the implementation of their functions and responsibilities, it is also necessary to regulate the independence and organizational support of officers. An example is the settings in the GDPR. In order to optimize the function of the data protection officer, the GDPR regulates how access and support must be provided by the organization to the data protection officer as stipulated in Article 38 GDPR. This includes arrangements regarding the independence of the data protection officer. Independence is necessary because the source of a data protection officer may originate from inside and outside the organization, including conflict of interest's issue. The existence of officers from inside and outside the organization is possible in the PDP Act or known through the data protection officer as a service. In addition,

it is also necessary to determine whether the Officer is a function that is only attached to one organization or can perform his functions cross-organizationally as an effort to provide the officer's function efficiently.

4. Personal Data Protection Supervisory Agency

Institutions have an essential function in the process of developing the protection of personal data. Although the institutional determination had been deadlocked in the discussion process, the institution was finally determined to be under the President as stipulated in Article 58 of the PDP Act. Each institution is always given the authority to carry out its functions and duties. Using the classification of data protection agency authorities in the GDPR, namely investigation power, corrective power and authorisation and advisory powers, institutional authorities reflect the three authorities with a focus point on the authority of the inves tigasi as described in the Table below.

Table 8 The Authority of the Personal Data Protection Supervisory Agency

Classification of Authority	Forms of Authority
Supervisory Authority	<ul style="list-style-type: none"> a. Policy formulation and determination; b. Compliance oversight of personal data controllers; c. Assessment of the fulfillment of data transfer requirements outside the territory of Indonesia.
Authority to Rectify	<ul style="list-style-type: none"> a. Imposition of administrative sanctions; b. Orders in the context of follow-up supervision of data controllers / data processors; c. Publication of the results of supervision.
Investigative Authority	<ul style="list-style-type: none"> a. Assisting law enforcement officials in handling suspected criminal acts of personal data ; b. Cooperate with other countries' Personal Data Protection agencies in cross-border breaches; c. Receive complaints and/or reports of alleged violations; d. Examination of complaints, reports, and/or supervisory results; e. Summon and present any person and/or public agency related to the alleged violation; f. Request information, data, information, and documents; g. Presenting experts in the examination; h. Inspection of electronic systems, facilities, spaces, and/or places used by the Personal Data Controller and/or Personal Data Processor, including gaining access to data and/or appointing third parties; and i. Request legal assistance to the prosecutor's office in dispute resolution.

Source: Author, 2022.

5. Penalty

The sanctions imposed for violations of the PDP Act are administrative sanctions. Administrative sanctions are imposed by the Personal Data Protection Supervisory Agency in the form of written warnings, temporary suspensions, deletion or destruction and/or administrative fines. The amount of administrative fines that can be imposed is a maximum of 2% of annual income or annual receipts for variable violations. In addition to administrative sanctions, the PDP Law also provides criminal sanctions for criminal acts of personal data, whether committed by individuals or corporations. In addition to imprisonment and fines, additional penalties are also provided as described in the Table below. Against corporations, criminal penalties are imposed on administrators, control holders, control givers, beneficial owners and/or corporations. Fines to corporations are subject to a maximum of 10 (ten) times the maximum fine and are subject to additional penalties. Administrative sanctions and criminal sanctions do not rule out the possibility for data subjects to file compensation claims for violations of processing their personal data as stipulated in Article 12 of the PDP Act.

Table 9 The Criminal Saction of Personal Data Breaches of the PDP Act

Action	Imprisonment	Criminal Fines	
Unlawfully collect personal data to benefit oneself/others which may result in loss of data subjects	Maximum 5 years	Maximum Rp.5 Billion	Additional Criminal: Deprivation of profits and/or property acquired or the results of criminal acts and payment of compensation
Unlawfully disclose personal data that does not belong to him	Maximum 4 years	Maximum Rp.4 Billion	Additional criminal corporations: a. Deprivation of profits/proceeds of wealth obtained from criminal acts;
Unlawfully use personal data that does not belong to him	Maximum 5 years	Maximum Rp.5 Billion	b. Freezing of all/part of the corporation's business;
Create fake personal data or falsify personal data with the intention of benefiting yourself / others which can result in harm to others	Maximum 6 years	Maximum Rp.6 Billion	c. Permanent prohibition of performing certain acts; d. Closure of all/part of business premises/activities; e. Carrying out neglected obligations; f. Payment of indemnity; g. License revocation; and/or

Criminal provisions in the protection of personal data are one of the new stages of legal protection of personal data in Indonesia. In the regulatory scheme of the ITE Act, losses suffered due to the use of personal data without consent are placed in a civil perspective with the submission of compensation by data subjects as stipulated in Article 26 paragraph (2) of the ITE Act. Criminal regulation in the ITE Act is placed on how the process of obtaining personal data is carried out such as illegal access in Article 30 of the ITE Act, transferring or transferring electronic information/documents unlawfully in Article 32 of the ITE Act and data manipulation in Article 35 of the ITE Act. The regulation of sanctions for criminal acts of personal data breach in the PDP Act directly refers to the activities of collecting and processing personal data without rights that are not carried out based on the principles and provisions of personal data protection as stipulated in the PDP Act. Of course, further discussion is needed regarding criminal sanctions in the PDP act in the level of synchronization and implementation.

III. CONCLUSION

The PDP act as a regulation that specifically regulates the protection of Indonesian personal data in principle contains the regulation of components in the personal data protection ecosystem, namely data subjects, data controllers and data processors, data protection officers and data protection agencies. Referring to the composition of the regulatory structure, the PDP Act tends to regulate the processing of personal data more, in particular the obligations of data controllers and data controllers processor. The principles used in the PDP Act reflect the principles of international protection of personal data, namely the OECD Privacy Framework . The subject of regulation of personal data is the public and private sphere, including international organizations. The balance between the protection of individuals and the public interest colours the arrangements in the PDP Act which are reflected in the principles underlying the PDP Act. In the norm structure, efforts to balance the two things are raised in the exceptions to the applicability of the provisions of the PDP Law such as the exercise of data subject rights and notification of failure of personal data protection. The balance needs to be carefully observed in its implementation so as not to injure the spirit of protection of data subjects as part of the human rights. As a compact regulation, technical direction is required at the level of implementing regulations and regulations made by personal data protection supervisory agencies. Sanctions for violations which include administrative sanctions, especially fines, and criminal sanctions require study in their implementation, both in terms of procedural law and its implementation considering that the public sector is the subject of regulation of the PDP Act. Various implementing regulations and socialization programs including infrastructure strengthening need to be issued immediately following the promulgation of the PDP Act. The spirit of personal data protection as a preventive effort must be put forward before repressive efforts are used.

REFERENCES

- BBCNews. (2022, September 20). *DPR sahkan UU Perlindungan Data Pribadi*. Retrieved September 25, 2022 from <https://www.bbc.com/indonesia/articles/cp6l1396y91o>
- Breitbarth, P. (2018, Agustus 28). <https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/>. From <https://iapp.org/news/a/on-large-scale-data-processing-and-gdpr-compliance/>
- Burhan, F. A. (2021, Juli 3). From <https://katadata.co.id/yuliawati/digital/60dfc13d1340f/ruu-pdp-molor-dpr-dan-kominfo-beda-pandangan-soal-lembaga-independen>
- Data Pribadi, K. P. (2018, Oktober 18). From <https://id.safenet.or.id/2018/10/rilis-pers-ruu-perlindungan-data-pribadi-penting-menjadi-prioritas-prolegnas-2019/>
- Dirjen IKP, K. C. (2014). *Naskah Akademik Rancangan Undang-undang Perlindungan Data Pribadi*. Jakarta. From https://www.bphn.go.id/data/documents/na_perlindungan_data_pribadi.pdf
- ELSAM. (2016). *Perlindungan Data Pribadi di Indonesia-Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia*. Jakarta: ELSAM.
- Jayani, D. H. (2021, September 7). From <https://databoks.katadata.co.id/datapublish/2021/09/07/pencurian-data-pribadi-makin-marak-kala-pandemi>
- Kominfo. (2022, September 22). From [https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu_pdp/#:~:text=Jakarta%2C%20Ditjen%20Aptika%20%E2%80%93%20Rancangan%20Undang,20%2F9%2F2022\)](https://aptika.kominfo.go.id/2022/09/rapat-paripurna-dpr-sahkan-ruu_pdp/#:~:text=Jakarta%2C%20Ditjen%20Aptika%20%E2%80%93%20Rancangan%20Undang,20%2F9%2F2022))
- Komunikasi, K. I. (2021). *Grand Design Pembentukan Ekosistem Data Protection Officer (DPO) Indonesia*. Jakarta: Kominfo.
- M.Ramli, A. (2022, September 25). From <https://nasional.kompas.com/read/2022/09/25/13335721/tafsir-uu-perlindungan-data-pribadi-yang-perlu-diketahui>
- OECD. (2013). *The OECD Privacy Framework*. Online: OECD. From https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
- Party, D. P. (2017). *Guidelines on Data Protection Officers ('DPOs')*. Brussel: Data Protection Working Party.
- Turku, & Helga. (2020, Juni 23). <https://iapp.org/news/a/how-to-ensure-you-appoint-an-independent-dpo/>. From <https://iapp.org/news/a/how-to-ensure-you-appoint-an-independent-dpo/>