# Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia

Russel Butarbutar[1*]

[1]*Faculty of Law, University of Indonesia, Depok, 16424, West Java, Indonesia*
[*]*Corresponding author. Email: russelbutar@gmail.com*

**ABSTRACT**
The issue of privacy and personal data protection has often made headlines in recent years, especially in the context of social networking, consumer profiles by online advertising companies, and cloud computing. In Indonesia through the EIT Law and MoCI Regulation 20 have not been comprehensively able to answer the challenges of protecting personal data. While other countries such as Singapore and Malaysia have arranged it with the help of the Authority established to resolve national and international issues related to the protection of personal data. In this study, it was found that data protection challenges include the unclear principle of data protection in Indonesia, the terminology of personal data, sensitive personal data, and the responsibility of service providers and data users. For this reason, Indonesia requires personal data protection laws which regulate: (1) All principles and terminology relating to data protection, sensitive data, cross-border flow of personal data, crimes against personal data, big data, cloud computing, and data related to artificial intelligence. (2) All violations must be threatened with fines and criminal threats that show seriousness in preventing violations of the law against a person's personal data. (3) Establishment of a Primary Authority that handles the protection of personal data and will represent the Government of Indonesia internationally on issues related to data protection.

***Keywords:*** *initiating, regulations, personal data protection, Indonesia*

## 1. INTRODUCTION

Electronic system users in conducting electronic transactions that use electronic systems carried out by electronic providers whose input or output can be in the form of electronic information and documents [1]. At present, we live in an era of "big data" [2]. Data has become the raw material for production and a new source of great economic and social value. Advances in data mining and analytics and large increases in computing power and data storage capacity have grown, with an order of magnitude, the scope of information available to businesses, governments, and individuals. The volume of data stored and generated in the world is growing so fast that scientists have to come up with new terms, including zettabytes and yottabytes, to describe the flood of data [3].

Society is increasingly dependent on information, which can be processed automatically without human intervention to produce machine functions, or produce further information or knowledge which can then become the basis for machines or actions that come from humans [4].

But on the other hand, with the increasing number of mobile and internet users there have been several cases relating to personal data leakage and leading to fraud or pornography. this fact reinforces the discourse about the importance of the rule of law for the protection of personal data [5]. Now, these issues are related to privacy and data protection issues in the context of social networking, online advertising consumer profiles, and cloud computing [6]. The threat to privacy and data protection no longer recognizes national borders because the world is connected and technology is complex [7] with the participation of most people [8].

Personal data protection is related to the concept of privacy which is an idea to maintain personal integrity and dignity. The right to privacy gives individuals the freedom to determine who holds information about them and how the information is used [8]. Whether it's information about personal data or other information that is owned that is likely to be accessed by the organization [9]. Personal data is any information relating to living or identified individuals [10] that sometimes competes with the collective interests of the community which sometimes justifies privacy restrictions [11].

The development of artificial intelligence, the Internet of Things, big data as a technology application related to personal data. For this reason, OECD [12] and APEC [13] can help create certainty and a supportive environment for businesses, especially regarding adequate consumer data protection [14].

In Indonesia, companies like Google, Go-Jek, Grab don't only provide services from users. However, they also collect the personal data of their users [15]. Companies, individuals and governments can collect personal data. Meanwhile, Indonesia does not have comprehensive personal data protection laws or regulations. Online lending platforms or P2P lending use the application to access and retrieve contact numbers from the debtor's cellphone. The online lending platform uses this personal contact to embarrass the borrower if they fail to pay their debts [16].

Of course, the development of technology and law are two very important variables in this era [17]. This raises general questions about how the principles of data protection, whether the legal rules on data protection in Indonesia are sufficient to protect electronic system users, how the challenges of data protection are faced, and how should the legal rules on data protection be designed to optimize electronic system users.

This research needs to be done to see and analyze the legislation related to personal data protection by looking at the comparison of regulatory perspectives in various countries such as Malaysia, Singapore, and the European Union. In Indonesia, at present, personal data protection is only regulated based on the Minister of Communication and Information Regulation Number 20 of 2016 concerning the Protection of Personal Data in the Electronic System [18].

### *1.1 Methodology*

This research was conducted by applying a comparative study [19] with Singapore, Malaysia to find out the development of regulations regarding the protection of personal data and get the best input in the initiation of the Law on the Protection of Personal Data in Indonesia.

### *1.2 Paper Structure*

After the introduction, section 2 (background) will discuss the principle of data protection; data Protection in Indonesia, and in section 3 (results) discuss the exsistence of data protection laws in various jurisdiction; and challenges in the formulation of personal data protection law in Indonesia. In the end, will present some closing notes from this paper.

### *1.3 Our Contribution*

Our main contribution is to look qualitatively and comparatively about the data protection laws in various jurisprudence (Malaysia, Singapore) to contribute in formulating personal data protection laws in Indonesia.

## 2. BACKGROUND

### *2. 1. The Principle of Data Protection*

The principle of protection arrangements applies to personal data [20], whether in the public or private sectors, which, because of the way they are processed, or because of their nature or the context in which they are used, risks privacy and personal freedom [12]. They should not be interpreted: as preventing the application of various protective measures for various categories of personal data, depending on nature and context in which they are collected, stored, processed or disseminated; or in a way that also limits freedom of expression [12]. The principles and rules regarding the protection of individuals relating to the processing of their data must, whatever their nationality or residence, respect their basic rights and freedoms, especially their right to protect personal data. This regulation is intended to contribute to the fulfillment of the fields of freedom, security and justice, and economic unity, for economic and social progress, for strengthening and economic convergence in internal markets, and o the well-being of natural persons [21].

Personal data processing must be designed to serve humanity. The right to protection of personal data is not absolute; it must be considered with its function in society and balanced with other fundamental rights, by the principle of proportionality. This regulation respects all basic rights and observes freedom and principles recognized in the Charter as enshrined in the Agreement, in particular respect for personal and family life, home and communication, protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct business, the right to effective remedies and fair trial, and cultural, religious and linguistic diversity [22].

Data protection principles as fundamental rights include: privacy, autonomy, transparency, non-discrimination [23].

### *1.1.1 Privacy*

Data protection has always been linked to privacy in such a way that it is very difficult to assess its very notion, its purpose, and its value without falling back to privacy [24]. Privacy can be defined in various ways, e.g. as the right to the confidentiality of communication, the right to be left alone, the right to control one's own life or the right to protect personal data. Privacy also illustrates an important aspect of tension between individuals and the community [25].

According to Shoeman, privacy has been determined based on the following different and different perspectives [26].

- Privacy as a claim, namely the right of individuals to determine information about what can be communicated to others.

- Privacy as a measure of control a person has: information about one's own; the intimacy of personal identity; or who have sensory access.
- Privacy as a condition or limited access to someone. Having privacy more than anyone else has limited access to information about it.

Likewise, according to the Black Law Dictionary [26]," *privacy is a condition or condition that is free from public attention to interference or interference with one's actions or decisions. Privacy is divided into two types, namely privacy autonomy and information privacy. Privacy autonomy is the right of an individual to regulate his personal activities or private decisions without interference, monitoring, or outside intrusion. While the privacy of information (tort) is the right of individuals to choose to determine whether, how and using where information about themselves is communicated to others, specifically. sensitive and confidential information."*

Privacy is considered important because it involves a protected individual, such as defamation, ridicule, harassment, manipulation, extortion, theft, subordination, and exclusion [27]. Developments and changes related to data and privacy are the results of complex interplays and related articulations, sometimes very heterogeneous, factors and actions, where moments and locations of choice and results are diverse, disseminated, and difficult to find. Meanwhile, in practice, privacy is a concept based on people's perceptions of interests and benefits [27].

### *1.1.2 Autonomy*

Laws, therefore, which limit the exercise of individual choices are generally framed carefully to ensure that they can maximize individual freedom. This serves two purposes. First, it recognizes respect for autonomy, and secondly, it allows for the development of the concept of privacy, where individuals are free from state control and control [28]. Recital 7 of the GDPR notes that '[n]atural persons should have control of their own personal data.' The principle of autonomy and the related focus on consent is also clearly linked to the concept of dignity [29]. Autonomy is the right of self-government. The fact that is happening now is that there are violations of democratic principles and the rule of law: data collection, exchange, and processing have the potential to damage central values such as individual autonomy and self-determination of information as well as the basic rights of privacy, data protection, and non-discrimination [30].

### *1.1.3 Transparancy*

Transparency is openness; clarity, lack of guile and attempts to hide damaging information. The word is used of financial disclosures, organizational policies and practices, lawmaking, and other activities where organizations interact with the public [26]. Recital 58 of the GDPR explicitly links this requirement to 'the principle of transparency'. This formulation is 'information-forcing' and addresses the imbalance of power, insofar as it 'force[s] the disclosure of information about data transfer and use'[29]. Data protection law however is made to ease the free flow of information by safeguarding personal data. In this respect privacy is a matter of opacity while data protection is related to transparency [30]. Increased transparency and control of their personal data in the right hands will increase user confidence. As a result, users will be more willing to share personal information, knowing exactly what will be used for and how much control they have over their data [31].

### *1.1.4 Non Discrimination*

The right to protection of personal data and non-discrimination interact in different ways and there is a need to increase its effectiveness. Regarding data processing technology, there are two complementary aspects of data protection and non-discrimination rights, namely the type of data covered by the protection and the type of control provided [32]**.** The principle of non-discrimination related to automated data processing techniques can be applied to a large amount of information available to build profiles (individuals and groups) that can be used to treat people differently, which makes it easier to carry out large-scale, careful discrimination [32]. For non-discrimination provisions to apply, it is sufficient that there are (1) differences in treatment (2) between 'people' or 'groups of people' in 'analogies' or 'relevant similar situations' (3) without 'objective and reasonable justification'[33] .

## *2. 2. Data Protection in Indonesia*

Law Number 11 of 2008 which is amended by Law Number 19 of 2016 concerning Electronic Information and Transactions (EIT Law) consists of 12 Chapters and 54 Articles. Chapter 1 (Articles 1-2) regulates general provisions. Chapter 2 (Articles 3-4) regulates principles and objectives, Chapter 3 (Articles 5-12) regulates information, documents, and electronic signatures; Chapter 4 (Articles 13-16) regulates the Implementation of electronic certification and electronic systems. Article 15 regulates the obligations and responsibilities of each electronic system operator must operate the electronic system reliably and safely and is responsible for the operation of the electronic system as it should with exceptions if the Electronic System Operator can prove the occurrence of force, error, and/or negligence of the users of the System Electronic. Chapter 5 (Articles 17-22) regulates electronic transactions. Article 21 paragraph 2 regulates the parties responsible for all legal consequences in implementing electronic transactions provided that: (1) if done alone, all legal consequences in the implementation of electronic transactions are the responsibility of the parties to the transaction; (2) if done through the granting of power of attorney, all legal consequences in implementing electronic transactions are the responsibility of the grantor; or (3) if done through an electronic agent, all legal consequences in the implementation of electronic transactions are the responsibility of the electronic agent organizer [34].

Chapters 6 (Articles 23-26) regulate domain names, intellectual property rights, and protection of personal rights. Chapter 7 (Articles 27-37) regulates prohibited acts. Article 27 prohibits distributing possessions that violate decency. Article 28 prohibits the distribution of false and misleading news. Article 29 prohibits sending information containing threats of violence or intimidation that is intended in private. Article 30 regulates the prohibition on accessing another person's computer and/or electronic system by any means including breaking into the security system. Article 31 regulates the prohibition of interception of information and electronic documents belonging to others without rights and against the law. Article 32 contains a prohibition on the transfer of information and electronic documents belonging to another person without rights. Article 33 prohibits any actions which disturb the electronic system. Article 34 prohibits the production, import, distribution, supply or possession of hardware or software developed to facilitate the acts referred to in Article 27 to Article 33. Article 35 prohibits the manipulation or falsification of electronic documents. Article 36 prohibits the provisions referred to in Articles 27-34 which result in harm to others [34].

Chapter 8 (Articles 38-39) regulates dispute resolution including a lawsuit to the court. Chapter 9 deals with the role of government and the role of the community (Articles 40-41). Chapter 10 on investigations (Articles 42-44) regulates the investigation and evidence of the investigation, prosecution, and examination of the court hearing. Chapter 11 concerning criminal provisions (Articles 45-52). Article 45 stipulates that the maximum threat of imprisonment is 12 years and a fine of 2 billion rupiahs for the act of sending information containing threats of violence or intimidation that are addressed in person (Article 29). While Article 51 provides maximum imprisonment of 12 years imprisonment and/or a maximum fine of 12 billion rupiahs for acts that violate Article 35 and Article 36. Chapter 12 (Article 53) concerning transitional provisions and Chapter 13 (Article 54) concerning closing provisions [34].

Furthermore, the regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning the protection of personal data in the electronic system (MoCI Regulation 20) is issued as mandated under Article 15 (3) Government Regulation No. 82 of 2012 concerning Application of Systems and Electronic Transactions (GR 82) [35]. MoCI Regulation 20 consists of 12 Chapters and 39 Articles. Chapter 1 (Article 1-2) concerning general provisions relating to personal data, certain personal data, the owner of personal data, the approval of the owner of personal data, electronic systems, electronic system operators, users of electronic systems, business entities, ministers, and director-general. Article 2 regulates the protection of personal data in electronic systems including protection of the acquisition, collection, processing, analysis, storage, announcement, transmission, distribution and destruction of personal data. For this reason, all processes must be carried out based on the principle of protecting personal data in the form of respect for privacy; confidential under the agreement, based on the agreement, the relevance of the objectives of acquisition, collection, processing, analyzing, storing and disseminating; electronic system feasibility; good intention; the availability of internal rules for managing personal data protection; responsibility for the mastery of personal data; ease of access and correction of personal data by the owner of personal data; integrity, accuracy, and validity and updating of personal data [36].

Privacy is the freedom of the owner of personal data to declare confidentially or not reveal the confidentiality of his personal data, unless otherwise specified by law (Article 2 paragraph (3)). Consent must be given or confirmed by the owner of personal data regarding the truth, confidentiality status, and purpose of managing personal data. Besides validity becomes an important point relating to the legality in the acquisition, collection, processing, analyzing, sending, disseminating, and destroying personal data [36].

Chapter 2 (Articles 3-25) concerning the protection which contains the protection of personal data in the electronic system in the process of acquiring, collecting, processing, analyzing, sending, distributing, and destroying personal data. The electronic system used must be certified and each provider of the electronic system must have internal rules to implement the process of protecting personal data, and have a mechanism regarding the prevention of failure in data protection. Providers of electronic systems must also provide consent forms in the Indonesian language to seek approval from the owner of personal data [36].

Chapter 3 concerning the rights of the owner of personal data (Articles 26-28), namely: the right to the confidentiality of personal data; filing complaints; get access to change or update his personal data; access to historical data; requesting the destruction of certain individual data. Chapter 4 regarding users' obligations (Article 27) consists of obligations: maintaining the confidentiality of personal data in its possession, using personal data under user needs only, protecting personal data from misuse; and personal or organizational responsibility for overcoming personal data in its possession. Chapter 5 (Article 28) concerning the obligations of electronic system operators: undertaking electronic system certification; maintain data protection; written notification to the owner of personal data in case of failure to protect confidential personal data; have internal rules related to data protection; provide an audit track record of activities; gives the owner of personal data an option about the data he manages or the consent of the owner of the personal data; giving access and opportunity for the owner of personal data to change and update his personal data; provide a contact person to contact the owner of personal data [36].

Chapter 6 on dispute resolution (Articles 29-33) which regulates the mechanism of complaints by the owner of personal data directly to the Minister. Dispute resolution is prioritized deliberately and administratively. Even claims related to personal data protection are only in the form of civil lawsuits (Article 32). Chapter 7 deals with the role of government and society (Article 34). Chapter 8 (Article 35) concerning supervision. Supervision is carried out by the Minister with the delegation of authority to the Director-General. Chapter 9 (Article 36) concerning administrative sanctions. Administrative sanctions will be given to parties who obtain, collect, process, analyze, store, display, announce, send, and/or disseminate Personal Data without the right to be subjected to administrative sanctions under statutory provisions in the form of (1) oral warnings; (2) written warning; (3) temporary suspension of activities; and/or (4) announcements on online sites. Chapter 10 is about other provisions (Article 37), and Chapter 11 (Article 38) concerning transitional provisions [36].

Based on the above regulations, MoCI Regulation 20 does not clearly and strictly regulate the protection of personal data. This rule is only normative and tends to be administrative, including sanctions if breaches of data protection are only administrative.

It must be admitted that the processing of personal information has been adopted by the MoCI Regulation 20 which has followed certain general principles in GDPR relating to the processing of personal information, among others: validity, confidentiality, purpose of limitation, accuracy and restriction of storage [35].

# 3. RESULTS

## *3.1. Exsistence of Data Protection Laws in Various Jurisdiction*

### *3.1.1 Malaysia*

In Malaysia, laws governing the protection of personal data have been enacted since the late 1990s. The first draft of the country's Personal Data Protection Bill ('PDP Bill') was released for public consultation in 2000. A series of campaigns and roadshows were held throughout the country to explain the reasons for and importance of the PDP Bill. Exceptional responses were given by the community, especially from individuals, companies, consumer associations, non-governmental organizations [37].

The first comprehensive personal data protection law in Malaysia was passed by the Malaysian Parliament on 2 June 2010 and entered into force on 15 November 2013, called the Personal Data Protection Act 2010 (PDPA). This PDPA gives meaning Personal data means all information relating to commercial transactions, namely: (1) processed in part or in full using equipment that operates automatically in response to instructions given for that purpose; (2) recorded with the intention that it must be partly whole or processed using said equipment, or (3) recorded as part of a relevant filing system or with the intention that it must form part of a relevant filing system, and, in each case [38]. Including those that relate directly or indirectly to the data subject, which is identified or identified from that information or from it and other information that is owned by the data user.

Personal data includes sensitive personal data or expressions of opinion about the subject of data. Excluded for data processed for credit reporting business purposes carried out by credit reporting agencies under the 2010 Credit Reporting Agent Act [38].

The data protection principles in PDPA [39] in sections 5-12 include the seven principles plus data subject rights which are mostly adopted from the EU Data Protection Directive, which consists of general principle processing with consent; other general processing limitation-lawfulness; necessary and not excessive; collection and notice principles; use and disclosure principles. This limitation on disclosure by data users is supported by violations committed by third parties who collect, or disclose, or sell personal data held by data users unless they can show that they act in conditions that justify their actions. For sensitive personal data, security principle; data retention principle and rights to blocking processing; data integrity principle; access and correction principle [40].

Meanwhile, personal data consisting of information on physical or mental health or condition of a data subject, political opinions, religious beliefs or other similar beliefs, commission or alleged commission by violations or any personal data determined by the Minister of Communication and Multimedia (Minister ) based on published orders called 'sensitive personal data' [38].

For electronic marketing activities that involve processing personal data for commercial transactions. There are no specific provisions in PDPA relating to electronic marketing. Direct marketing 'means communication in any way from any advertising or marketing material aimed at specific individuals [41].

For compliance with PDPA, companies are required to manage personal data and other information from clients. They must conduct business under PDPA requirements, including the life cycle management of personal data from the point where personal data is collected, used, stored and destroyed. Thus a central repository may be required for approval management [42].

Meanwhile, the effectiveness of PDPA is required for data users in three situations. First, data users are established in Malaysia. Second, the processing is carried out by people employed or employed by data users in Malaysia. Third, if the data user is not established in Malaysia, but uses tooling to process personal data in Malaysia [43].

As an Authority, to implement the PDPA provisions, a Commissioner for Personal Data Protection (Commissioner) must be appointed. The Personal Data Protection Advisory Committee which will be appointed by the Minister is responsible for advising the Commissioner. The Personal Data Protection Advisory Committee consists of one Chairperson, three members from the public sector, and at least seven, but no more than eleven other members with terms of office will not exceed three years; however, members can be appointed for two consecutive periods.

Decisions of the Commissioners can be appealed through the Personal Data Protection Court of Appeals. The following are examples of decisions that can be appealed [44]:

- Part II Division 2 PDPA, or decisions relating to data user registration.
- Section 23 (5) of PDPA, or the Commissioner's refusal to register a code of practice.
- Section 108 PDPA, or law enforcement notification services.
- Section 109 of PDPA, or the Commissioner's refusal to change or cancel an implementation notice.
- Section VIII of the PDPA, or the Commissioner's refusal to conduct or continue an investigation based on complaints.

Data users can continue to file a review of the decision in the Malaysian High Court if the data user does not agree with the decision of the Personal Data Protection Advisory Committee [44].

On the other hand, to deal with online privacy issues (including cookies and location data) there are no provisions in PDPA. However, the Commissioner may issue further guidance on this issue in the future and faithfully processing electronic data on personal data subject to PDPA [45].

### *3.1.2 Singapore*

Singapore enacted the 2012 Personal Data Protection Act ("PDPA") which regulates the collection, use, and disclosure of personal data by organizations. The Personal Data Protection Commission ("Commission") was established under PDPA with main functions, among others, to increase awareness of data protection in Singapore and manage and enforce PDPA. This law applies in three phases: *(1) p*rovisions relating to the formation of the Personal Data Protection Commission ("Commission") cam*e into force on January 2, 2013; (2) p*rovisions relating to the National Do-Not-Call (DNC) Registry come *into force on January 2, 2014; (3) t*he main data protection provisions come into force on July 2, 2014 [46]. The PDPA protection model balances "both the right of individuals to protect their personal data" against "the organization's need to collect, use or disclose personal data for legitimate and reasonable purposes" [47].

The DNC was issued to avoid the effects of increasing dependence on personal smart devices and more aggressive digital marketing strategies adopted by many organizations [48]. PDPA contains two (2) sets of main provisions, which include data protection and a Do Not Call (DNC) registry, which must be met by the organization. In brief, data protection provisions deal with the following [49]:

- Having a reasonable purpose, notifying the purpose and getting approval for the collection, use or disclosure of personal data;
- Allow individuals to access and correct their personal data;
- Managing personal data (relating to ensuring accuracy), protecting personal data (including protection in the case of international transfers) and not storing personal data if no longer needed; and
- Have policies and practices to comply with PDPA.

The PDPA's DNC Registry provisions are set out in Part IX of the PDPA (the "DNC Provisions"). These deal with the establishment of Singapore's national DNC and the obligations of organisations relating to the sending of certain marketing messages to Singapore telephone numbers. The DNC will initially comprise three (3) separate registers kept and maintained by the Commission under section 39 of the PDPA (the "DNC Registers") which cover telephone calls, text messages and faxes. Users and subscribers will be able to register their Singapore telephone number(s) on one or more DNC Registers depending on their preferences in relation to receiving marketing messages through telephone calls, text messages or faxes [50].

In this case, the organization has the following obligations about sending certain marketing messages to Singapore telephone numbers [51]: (1) Checking the relevant DNC Register(s) to confirm if the Singapore telephone number is listed on the DNC Register(s); (2) Providing information on the individual or organization who sent or authorised the sending of the marketing message; and (3) Not concealing or withholding the calling line identity of the sender of the marketing message.

PDPA establishes a general data protection regime, which consists of nine data protection obligations imposed on the organization, namely: (1) consent obligation; (2) purpose limitation obligation; (3) notification obligation; (4) access and correction obligation; (5) your business must also correct errors or omissions in the personal data that is in its possession upon request unless it is reasonable to not make the correction; (6) accuracy obligation; (7) protection obligation (8) retention limitation obligation; (9) transfer limitation obligation; (10) openness obligation [49].

In realizing the steps to implement PDPA, with the appointment of ministers from the Personal Data Protection Commission (PDPC) to manage PDPA and the Data Protection Advisory Committee to advise the Commission. PDPA only covers the private sector, and even then with many exceptions. Data protection provisions come into force in July 2014, while DNC provisions (come into force in January 2014) [40].

The PDPC regularly publishes decisions relating to organizations that are found to have contravened the data protection provisions under the Personal Data Protection Act (PDPA). These decisions provide salient insights which organizations are strongly encouraged to take guidance from and to implement measures to prevent similar occurrences. They also serve to remind individuals and organizations of their respective rights and obligations under the PDPA. In the longer term, the publication of cases on the PDPC's website aims to promote accountability among organizations to safeguard consumer interest and trust [52].

### *3.2. Challenges in the Formulation of Personal Data Protection Law in Indonesia*

Increasing business through the internet (IoT) is changing the mindset and need for personal data protection. IoT businesses must devise a privacy alignment strategy for their products or services by including in their design the privacy and data protection capabilities needed for compliance with regulations and gain user trust [53]. Especially for P2P lending, it is already sufficient to provide legal protection for both organizers and users [54].

In Indonesia, according to MoCI Regulation 20, if the owner of personal data suffers a loss then he can report his case to the Minister with the help of the Aptika Director-General. But the question is, when will someone realize that his personal data is being used by someone else against the law? Then, what kind of loss is meant in this MoCI Regulation 20? How does one judge that his data has been misused in another form, for example, it has become a form of Big Data or used by third party? [55] Where is the data limitation is private data (validation data) or data that has been legitimized for further processing? Where is the limitation or category that the personal data is Personally Identifiable Information (sensitive data) or the data is not sensitive?[56]

When viewed from the burden of complaints (lawsuits), this is on the shoulders of a person whose personal data is used legally and the resolution is carried out by deliberation to reach consensus, and if for example my conduct can be detected, say in the country then only administrative sanctions can be given, what if the culprit not in the jurisdiction of Indonesian law, and they use these personal data for commercial or other malicious purposes, this is a critique that must be resolved in the future. The Ministry of Communication and Information should be responsible and have technological and legal mechanisms to maximize the protection and confidentiality of personal data someone likely to be abused by another party, be it in the context of seeking profit or other purposes.

For this reason, Indonesia must have legislation in the future in the context of protecting personal data. The urgency is not only in state sovereignty over data [57] but also for personal sovereignty over the data, and of course, it must consider the competition of data between countries to be very fierce going forward. Regarding competition policies, consumer policies, and data protection policies that are often at risk of privacy rights and individual privacy preferences [58]. It not only concerns administrative data, business but concerns crimes against personal data. This law must provide the person with privacy and freedom that his personal data is obtained and used for the true purpose of the owner's agreement, and not misused by other parties in a national or cross-border scope [59].

Future personal data protection arrangements must define all principles and terminology relating to data protection, sensitive data, transborder flows of personal data, crimes against personal data, big data, cloud computing, and data related to artificial intelligence. This law must be supplemented by a fine and a criminal threat that shows seriousness in preventing violations of the law against a person's personal data [60].

Indonesia must have a Primary Authority that handles the protection of personal data and will represent the Government of Indonesia internationally on issues related to data protection. This authority aims to balance the need to protect individual personal data and the organization's need to use data for legitimate purposes [61]. Later this Authority will work with relevant sector regulators in carrying out its functions, helping organizations adopt good data protection practices and helping individuals to better understand how they can protect their own personal data from misuse, and help organizations improve customer relationships by increasing customer trust.

## 4. CONCLUSION

Indonesia requires personal data protection laws that regulate: (1) All principles and terminology relating to data protection, sensitive data, cross-border flow of personal data, crimes against personal data, big data, cloud computing, and data related to intelligence artificial. (2) All violations must be threatened with fines and criminal threats that show seriousness in preventing violations of the law against a person's personal data. (3) Establishment of a Primary Authority that handles the protection of personal data and will represent the Government of Indonesia internationally on issues related to data protection.

## REFERENCES

[1] Indonesia, *Government Regulation Number 82 of 2012 concerning Implementation of Electronic Systems and Transactions*. .

[2] A. Cormack, “A data protection framework for learning analytics,” *J. Learn. Anal.*, vol. 3, no. 1, pp. 91–106, 2016.

[3] A. B. Munir, M. Y. S. Hajar, and F. Muhammad-Sukki, “Big data: big challenges to privacy and data protection,” *Int. Sch. Sci. Res. Innov.*, vol. 9, no. 1, 2015.

[4] S. Chalton, “A Thorogood Report: The Legal Protection of Databases,” London, 2001.

[5] BPHN, *Naskah Akademik RUU Perlindungan Data Pribadi*. Jakarta: BPHN, 2016.

[6] EDRi, “An Introduction to a Data Protection,” 2013.

[7] A. Mehmood, I. Natgunanathan, Y. Xiang, G. Hua, and S. Guo, “Protection of big data privacy,” *IEEE Access*, vol. 4, pp. 1821–1834,

2016.

[8] S. Gutwirth, Y. Poullet, P. De Hert, and R. Leenes, *Computers, Privacy and Data Protection: an Element of Choice*. Springer: SPringer Science+Business Media B.V, 2011.

[9] PDPC, “Overview: What is Personal Data.” [Online]. Available: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview. [Accessed: 02-Sep-2019].

[10] E. Commission, “What is personal data?” [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. [Accessed: 02-Sep-2019].

[11] W. J. Schünemann and M. O. Baumann, *Privacy, data protection and cybersecurity in Europe*. Springer International Publishing., 2017.

[12] OECD, “Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data,” 2013. [Online]. Available: www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. [Accessed: 02-Sep-2019].

[13] APEC, “APEC Privacy Framework,” 2015. [Online]. Available: https://www.apec.org/Publications/2017/08/APEC-Privacy-Framework-(2015). [Accessed: 02-Sep-2019].

[14] S. Yatim, “The privacy battle in Indonesia – the longer the battle, the more consumers stand to lose.” [Online]. Available: https://www.thejakartapost.com/academia/2019/02/21/the-privacy-battle-in-indonesia-the-longer-the-battle-the-more-consumers-stand-to-lose.html. [Accessed: 02-Sep-2019].

[15] T. Conversation, “Indonesia urgently needs personal data protection law.” [Online]. Available: http://theconversation.com/indonesia-urgently-needs-personal-data-protection-law-91929. [Accessed: 22-Aug-2019].

[16] T. J. Post, “Protecting personal data,” 2019. [Online]. Available: https://www.thejakartapost.com/. [Accessed: 22-Aug-2019].

[17] National Research Council (et al), *Technology, policy, law, and ethics regarding US acquisition and use of cyberattack capabilities*. National Academies Press, 2009.

[18] Indonesia, *Regulation of the Minister of Communication and Information Number 20 of 2016 concerning Protection of Personal Data in the Electronic System*. .

[19] P. Cruz, *Comparative Law in a Changing World*, Second. London: Cavendish Publishing Limited, 1999.

[20] R. Leenes, R. Van Brakel, S. Gutwirth, and P. (Eds. ). (2017). De Hert, *Data Protection and Privacy: The Age of Intelligente Machines*. Bloomsbury Publishing, 2017.

[21] *GDPR, Recital 2*. .

[22] *GDPR, Recital 4*. .

[23] Y. McDermott, “Conceptualising the right to data protection in an era of Big Data,” *Big Data Soc.*, vol. 4, no. 1, p. 2053951716686994., 2017.

[24] T. Maria, “Data protection as a fundamental right next to privacy?‘Reconstructing’a not so new right,” *Int. Data Priv. Law*, vol. 3, no. 2, pp. 88–89, 2013.

[25] et al Friedewald, Michael ., “Privacy, data protection and emerging sciences and technologies: towards a common framework,” *Innov. Eur. J. Soc. Sci. Res.*, vol. 23, no. 1, pp. 61–67, 2010.

[26] et al. . Garner, Bryan A., *Black’s law dictionary*. 2004.

[27] M. Petkovic and W. (Ed. . Jonker, *Security, privacy, and trust in modern data management*. Springer Science & Business Media, 2007.

[28] S. A. McLean, *Autonomy, consent and the law*. Routledge, 2009.

[29] Y. McDermott, “Conceptualising the right to data protection in an era of Big Data,” *Big Data Soc.*, vol. 4, no. 1, 2017.

[30] S. Gutwirth, R. Leenes, and P. De Hert, *Data Protection on the Move - Current Developments in ICT and Privacy/Data Protection*, vol. 24. Springer: SPringer Science+Business Media B.V, 2016.

[31] M. Nati, “Personal Data Receipts: How transparency increases consumer trust,” 2018. [Online]. Available: https://assets.ctfassets.net/nubxhjiwc091/6LIJp62XscyqI6OcweoSiy/5522b10976e57f20de4966bcafdd006a/Personal_Data_Receipts_r1.5_2.pdf. [Accessed: 22-Dec-2019].

[32] et al. (ed. ). Gutwirth, Serge, *European data protection: in good health?* Springer Science & Business Media, 2012.

[33] M. Hildebrandt and S. Gutwirth, *Profiling the European citizen*. Dordrecht: Springer, 2008.

[34] Indonesia, *Law Number 11 of 2008 which is amended by Law Number 19 of 2016 concerning Electronic Information and Transactions*. .

[35] Asketlaw.com, “Data Protectioan & Privacy 2020.” [Online]. Available: https://aksetlaw.com/content/uploads/2019/09/Data-Protection-Privacy-2020.pdf. [Accessed: 07-Nov-2019].

[36] Indonesia, *Minister of Communication and Information Technology Number 20 of 2016 concerning the Protection of Personal Data in the Electronic System*. .

[37] E. L. Y. Cieh, *Personal data protection and privacy law in Malaysia. In: Beyond data protection*. Springer, Berlin, Heidelberg, 2013.

[38] D. PIPER, “Data Protection Law of The World.” [Online]. Available: https://www.dlapiperdataprotection.com/index.html?t=definitions&c=MY. [Accessed: 20-Jan-2020].

[39] N. Ismaill, “Selected issues regarding the Malaysian Personal Data Protection Act (PDPA) 2010,” *Int. Data Priv. Law*, vol. 2, no. 2, p. 105, 2012.

[40] G. Greenleaf, “Malaysia: ASEAN’s First Data Privacy Act in Force,” 2014.

[41] D. PIPER, “Electronic Marketing.” [Online]. Available: https://www.dlapiperdataprotection.com/index.html?t=electronic-marketing&c=MY. [Accessed: 01-Dec-2019].

[42] Crown Records Management, “Personal Data Protection Act (PDPA) in Malaysia.” [Online]. Available: https://www.crownrms.com/intl/en-my/article/personal-data-protection-act--pdpa--in-malaysia. [Accessed: 05-Feb-2020].

[43] A. Rouhani and N. A. Manap, “The Impact of Cloud Computing on the Protection of Personal Data in Malaysia.”

[44] D. PIPER, “Data Protection Laws of the World.” [Online]. Available: https://www.dlapiperdataprotection.com/index.html?t=authority&c=MY. [Accessed: 07-Feb-2020].

[45] D. PIPER, “Online Privacy.” [Online]. Available: https://www.dlapiperdataprotection.com/index.html?t=online-privacy&c=MY. [Accessed: 10-Oct-2019].

[46] D. PIPER, “Law.” [Online]. Available: https://www.dlapiperdataprotection.com/index.html?t=law&c=SG.

[47] M. Yip, “Personal Data Protection Act 2012: Understanding the consent obligation,” *Pers. Data Prot. Dig.*, p. 266, 2017.

[48] W. B. Chik, “The Singapore personal data protection act and an assessment of future trends in data privacy reform,” *Comput. Law Secur. Rev.*, vol. 29, no. 5, pp. 554–575, 2013.

[49] Singaporelegaladvice, “Essential PDPA Compliance Guide for Singapore Businesses.” .

[50] Singapore, *PDPA, Section 2.4, Part 9*. .

[51] Singapore, *PDPA, Section 2.5*. .

[52] PDPC, “Data Protection Enforcement Cases.” [Online]. Available: www.pdpc.gov.sg/Commissions-Decisions/Data-Protection-Enforcement-Cases. [Accessed: 22-Aug-2019].

[53] A. Chauduri, “Internet of things data protection and privacy in the era of the General Data Protection Regulation,” *J. Data Prot. Priv.*, vol. 1, no. 1, pp. 64–75, 2013.

[54] L. Abubakar and T. Handayani, *Financial technology: Legal challenges for Indonesia financial sector*. IOP Conference Series: Earth and Environmental Science. IOP Publishing, 2018.

[55] T. Hasebe, R. Akiyama, and M. Yoshioka, “Electronic data protection system,” 1995.

[56] A. Narayanan and V. Shimatikov, “Myths and fallacies of" personally identifiable information",” *Commun. ACM*, vol. 53, no. 6, pp. 24–26, 2010.

[57] J. S. Bauchner, “State sovereignty and the globalizing effects of the Internet: A case study of the privacy debate,” *Brook. J. Int’l L.*, vol. 26, p. 689, 2000.

[58] W. Kerber, “Digital markets, data, and privacy: competition law, consumer law and data protection,” *J. Intellect. Prop. Law Pract.*, vol.

11, no. 11, pp. 856–866, 2016.

[59] L. Ryz and L. Grest, “A new era in data protection,” *Comput. Fraud Secur.*, vol. 3, pp. 18–20, 2016.

[60] S. H. Kadish, “Some observations on the use of criminal sanctions in enforcing economic regulations,” *Univ. Chicago law Rev.*, vol. 30, no. 3, pp. 423–449, 1963.

[61] PDPC, “Overview.” [Online]. Available: https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview. [Accessed: 22-Dec-2019].