Corporate and Trade Law Review (CTLR)
Vol.1, No.2, July-December 2021, pp. 98-118
ISSN: 2807-7644 | https://journal.prasetiyamulya.ac.id/

Privacy and Data Protection: Indonesian Legal Framework

Brahmantyo Suryo Satwiko
Tilburg University, The Netherlands

Article Info

Keyword:

data protection regime; data collection and processing; data protection issues; data protection legislation

ABSTRACT

Due to technological advancement, the utilization of internet and mobile connections in Indonesia to perceive rapid growth in recent years. A major development in particular lies within the field of e-commerce, marketplace, and digital portal applications. Extensive advancement within the abovementioned fields led to the involvement of the Indonesian government and private companies in which collecting and processing Indonesian citizens' personal data took place. Multitude issues relating to data protection regimes arose due to such acts as Indonesian data protection legislations are considered inadequate for their overlapping and vague aspects. These issues obtained numbers of apprehension from the Indonesian government as well as experts within this field with regard to the urgency of having a sufficient data protection law. Plenty of countries have competent data protection laws that have implemented the required elements, for instance, the European Union and Singapore. Accordingly, data protection laws from those countries will play an important role in providing a perfect example for the drafting of an advanced Indonesian data protection law that is uniform and encompassed all required aspects of data protection regimes without neglecting profound deliberation relating to the pitfalls.

ABSTRAK

Dikarenakan adanya perkembangan teknologi, pemanfaatan internet dan koneksi seluler di Indonesia mengalami pertumbuhan yang pesat dalam beberapa tahun terakhir. Perkembangan pesat khususnya ada pada bidang *e-commerce*, *marketplace*, dan *digital portal applications*. Kemajuan pesat terhadap bidang-bidang tersebut di atas menyebabkan keterlibatan pemerintah Indonesia dan perusahaan swasta di mana pengumpulan dan pengolahan data pribadi warga negara Indonesia berlangsung. Banyaknya isu yang berkaitan dengan rezim perlindungan data muncul dikarenakan undang-undang perlindungan data di Indonesia dianggap tidak memadai karena aspeknya yang tumpang tindih dan tidak jelas. Isu-isu ini mendapat banyak perhatian dari pemerintah Indonesia serta para ahli dalam bidang ini sehubungan dengan urgensi untuk memiliki undang-undang perlindungan data yang memadai. Banyak negara memiliki undang-undang perlindungan data yang kompeten yang telah menerapkan elemen-elemen yang diperlukan, misalnya, Uni Eropa dan Singapura. Dengan demikian, undang-undang perlindungan data dari negara-negara tersebut akan memainkan peran penting dalam memberikan contoh sempurna untuk penyusunan undang-undang perlindungan data Indonesia yang lebih mutakhir, seragam dan mencakup semua aspek yang diperlukan dari rezim perlindungan data tanpa mengabaikan pertimbangan mendalam yang berkaitan dengan kesulitan yang mungkin muncul.

Article History:

Received:
27 January 2021

Reviewed:
1 September 2021

Accepted:
11 November 2021

Published:
22 December 2021

Corresponding Author:

Email:
brampurwadi@gmail.com

INTRODUCTION

The number of internet users in Indonesia expands promptly which the number has reached 171.17 million. The highest number lies within the age range of 15-19 years old (91%) and 20-24 years old (88.5%). Meanwhile, the lowest number lies within the age range of 60-64 years old (16.2%) and above 65 years old (8.5%).[1] Rapid development in Indonesia likewise takes place within the fields of e-commerce, marketplace, and digital portal applications in which a huge amount of foreign as well as domestic investment is poured into startups to monetize as well as obtaining profit deriving out of this flourishing sector. Furthermore, this leads to the involvement of the Indonesian government and private companies in data collecting and processing activities. Several activities that have been carried out include the collection of poverty data, population, economic census, disaster data, population identity data/*kartu tanda penduduk* (e-KTP), subscriber identification module (SIM) card registration for cellphone users, communication surveillance, and direct access to databases, smart city projects, election data collected through the voter registration process, medical records data and health insurance companies, financial and taxation data, whether it is collected by banking companies, financial services companies, insurance companies, or tax offices.[2]

However, at that moment, data collecting and processing were conducted under an insufficient data protection regime, hence many issues arose.[3] For instance, a personal data breach from the registration of mobile SIM cards occurred in early 2018 and there were more than 300 million numbers that had been registered when this case was discovered, breach of passenger data at Malindo Air in September 2019, the online lending platform provides whose licenses were revoked by the Financial Services Authority/*Otoritas Jasa Keuangan* (OJK)[4] along with Alert Task Force/*Satgas Waspada* Investasi throughout 2018 and 2019 for the misused of their platforms for accessing and retrieving information that was not included within the data collection agreement and it was for debt collection,[5] sales of personal data obtained from financial institutions, car, and property agents without the consent of data subjects,[6] and a breach relating to medical records for the first Indonesians confirmed case of COVID-19 virus in 2020.

It is undeniable that the idea of privacy is substantially harder to understand especially within the context of human rights. It is coherent that personal data shall be protected at all costs and within this case, individuals, government, and business organizations are the accountable ones. As privacy and data protection have been acknowledged for many years in Indonesia the crucial foundation that is enforced can be found within Article 28(G) of the 1945 Constitution of the Republic of Indonesia (Indonesian Constitution). The concept of privacy and data protection is not

[1] Dinita Andriani Putri, 'Personal Data Protection in Indonesia: The Long Road to Effective Implementation' [2019] World Wide Web Foundation.
[2] Wahyudi Djafar, 'Big Data dan Pengumpulan Data Skala Besar di Indonesia: Pengantar Untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi'.
[3] The data collection practices, as described above, significantly impact the magnitude of the threat of misuse of the collected personal data. The threat of misuse of collected personal data appears in the form of data breaches, unauthorized access of data, lack of proper lawful grounds for accessing data, and so on.
[4] OJK is an Indonesian government agency that regulates and supervises the financial services sector. The OJK is an autonomous agency designed to be free from any interference, having functions, duties, and powers to regulate, supervise, inspect, and investigate.
[5] Otoritas Jasa Keuangan (Financial Services Authority), 'Otoritas Jasa Keuangan dan BARESKRIM POLRI Sepakat Berantas Fintech Peer-To-Peer-Lending Ilegal dan Investasi Ilegal'.
[6] K&K Advocates, 'Unauthorized Transfer of Personal Data Might Be Punishable Under the Indonesian Criminal Law'.

mentioned precisely within the abovementioned article. However, it is applicable as the legal basis for further definite data protection laws and regulations.[7]

On the grounds that problems related to data protection rapidly increase Indonesian government took action by enacting the Law No. 11 of 2008 on Electronic Information and Transactions as amended by Law No. 19 of 2016 on Amendment of Law No. 11 of 2008 on Electronic Information and Transactions (collectively referred to as the EIT Law). Other relevant regulations were likewise implemented by the Indonesian government that includes the Government Regulation No. 82 of 2012 on the Implementation of Electronic Systems and Transactions (GR 82/2012) as amended by the Government Regulation No. 71 of 2019 on The Organization of Electronic Systems and transactions (GR 71/2019) and Minister of Communications and Informatics (MoCI) Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (MoCI 20/2016). However, the abovementioned regulations are deemed to be inadequate for their somewhat concise and unclear feature as it is not explicitly written and uncertain and thus incapable of protecting Indonesian citizens' personal data.

Moreover, the Indonesian data protection law regime is moving at a slow pace. Numbers of challenges are encountered by the Indonesian government within the enforcement of a comprehensive data protection law. Thus, it is pertinent to discover the best possible solutions and key provisions to solve any data security issues that may appear in the future. Additionally, a single unified and comprehensive regulation about personal data protection is nowhere to be found within the Indonesian legal system.[8] On top of everything, they are separated among several governmental and sectoral regulations which then caused an overlapping due to the fact that each sectoral regulation incorporates its own definition, specifically, within several aspects such as the purpose of personal data processing, notification or consent of the data subject, retention period of personal data, erasure or alteration of personal data, the disclosure of personal data to third parties, sanctions for violators of the relevant regulations, and recovery mechanisms for victims of privacy rights violations.[9]

The current existing overlapping regulations in Indonesia itself shall be contemplated as a regulatory challenge towards the implementation and enforcement of the prevailing data protection regime. This challenge raises several questions relating to the solutions and measures to overcome these issues as well as to avert possible challenges that might occur in the future that may include the incompetency of the policymakers in Indonesia to create an adequate regulation within the data protection regime because as Indonesian citizens the possibility of them being unfamiliar to a certain concept are relatively high. Thereupon, obtaining an in-depth awareness and knowledge relating to the aforementioned issues or challenges will be implied as institutional, social, and cultural challenges. By the same token, Indonesian experts and scholars, privacy advocates, and research institutions likewise hold a strong opposition towards the adequacy of Indonesian data protection laws due to their vast and obscure aspects.[10]

Conforming to the preliminary research a comprehensive and competent data protection regulation shall at least contain the principles of lawfulness, fairness, and transparency of processing, the purpose limitation principle, the data minimization principle, the data accuracy principle, the storage limitation principle, the data security principle, accountability principle, the independent

[7] Sinta Rosadi, 'Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia' (2018) 5 Brawijaya Law Journal 143.
[8] Sinta Rosadi, 'Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia' [2019].
[9] Djafar (n 2).
[10] Wahyudi Djafar, Benhard Ruben Fritz Sumigar, and Blandina Lintang Setianti, 'Perlindungan Data Pribadi – Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia' [2016] Seri Internet dan Hak Asasi Manusia.

supervision, data subject rights and their enforcement, obligations of controllers and processors, and international data transfers and flows of personal data.[11] Furthermore, many countries such as Brazil (Brazil's *Lei Geral de Proteção de Dados* (LGPD)), Thailand (PDPA), South Africa (South Africa's Protection of Personal Information Act (POPIA)), India, the European Union (General Data Protection Regulation 2016/679 (GDPR)), and Singapore (Singapore Personal Data Protection Act No. 26 of 2012 (PDPA)) have their own personal data regulations and they are likewise provided in detail.[12] GDPR and PDPA shall be the perfect example of data protection regulation due to their competency. Chiefly, the key provisions within their data protection regulation could barely be found within other countries' data protection regulation. The key provisions include the consent obligation, the purpose limitation obligation, the notification obligation, the access and correction obligations, the accuracy obligations, the protection obligation, the retention limitation obligation, the transfer limitation obligation, and the accountability obligation.[13]

Supplementary to the aforementioned aspects, PDPA implemented an unusual provision which is the Do-Not-Call (DNC) registry provision that basically forbids organizations from sending particular marketing messages to Singapore telephone and mobile numbers, fixed-line, residential, and business numbers that have been registered with the DNC registry.[14] This provides a great illustration in which business sectors likewise are referring to GDPR and PDPA in advancing their data protection regulations.[15] It is crucial for Indonesia to address urgently and promptly the need for a comprehensive and unified regulation concerning privacy and data protection. Hence, Indonesia must acquire insights from GDPR and PDPA to improve and face challenges in enforcing the data protection regime. Further discussions and elaboration in relation to the required elements within a new unified data protection regulation in Indonesia shall be provided consequently as the primary objective of this thesis. Moreover, personal data protection concepts that are regulated under the Indonesian laws and regulation within this present day, the relevancy of the implementation, challenges encountered throughout the enforcement of the current personal data protection regime in Indonesia, measures to address the abovementioned issues, and the knowledge from the EU's GDPR and Singapore's PDPA will be utilized as the bottom line in settling the inconsistencies within the current Indonesian data protection laws regime.

METHODS

The research will be conducted through doctrinal research, comparative research, and empirical research. Doctrinal research was preferred because the primary research questions along with sub-questions can solely be justified by utilizing systematic analysis towards legislation, case law, and literature. Through this method, data protection legislation in Indonesia will be assessed thoroughly starting from the end to the upper hierarchy which includes the 1945 Indonesian Constitutions and its amendments along with the Government Regulation and Ministerial Regulation. This method correspondingly plays a significant role within the study of relevant legal text, especially within the interpretation of the existing laws that are applicable for a specific circumstance.[16] Further examination will be conducted as well through the EU and Singapore data protection legislation as a comparative approach and the Indonesian legislation will be

[11] Chris Jay Hoofnagle, Bart Van Der Sloot, and Frederik Zuiderveen Borgesius, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65 <https://doi.org/10.1080/13600834.2019.1573501>.
[12] ibid.
[13] Personal Data Protection Commission – Singapore, 'Advisory Guidelines on Key Concepts in the Personal Data Protection Act'.
[14] ibid.
[15] Putri (n 1).
[16] Terry Hutchinson, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2016) 38 Erasmus Law Review.

distinguished and examine equally to classify the knowledge that will be beneficial for the policymakers in Indonesia. In addition, empirical research will function as the subject matter that relies on observation and experience.[17] It will assist the assessment of risks and challenges encountered by the Indonesian government within the enforcement of the data protection regime along with discovering suitable measures that can be taken by the Indonesian government in managing such risks and challenges. Furthermore, it will be in line with the relevant court cases and news reports from both printed and online media sources.

RESULTS AND DISCUSSION

1. The Concept of Personal Data Protection Under the Indonesian Laws and Regulations

1.1. Introduction

Originally protection of personal data is deliberated as an expansion from the right to privacy and within the Indonesian Constitution itself, this concept has been acknowledged and protected inside the general scope of human rights. EIT Law was then enforced in favor of regulating internet and electronic transaction-related activities. However, there is an absence of explicit provisions concerning personal data protection. Furthermore, personal data is regulated under Article 26(1) of the EIT Law with several supporting regulations such as MoCI 20/2016 that came into force in December 2018 and is only applicable for Personally Identifiable Information (PII) stored in electronic systems,[18] Article 15(3) of GR 82/2012, and GR 71/2019. There are around 30 statutory regulations at the very least that acknowledge the concept of privacy data protection whether in an explicit nor implicit way.

1.2. Sectoral Laws and Regulations

Indonesian legal system does not have a comprehensive and unified regulation relating to personal data protection as it is separated within several sectoral regulations, unlike the EU's GDPR. Besides the other 30 regulations mentioned above, EIT Law, MoCI 20/2016, and GR 71/2019 are solely applicable towards all data processing or usage of personal data within the electronic form by Electronic System Providers (ESPs). Although it is not applicable for personal data within a manual record, nevertheless it is accountable to adhere to the relevant regulations aside from the type of organizations. Moreover, Indonesia ratifies the consent-based regime as the primary principle in obtaining and processing personal data through electronic systems, and consent of the data is irrelevant unless required by the law or if the personal data was transferred publicly through electronic systems for public services. Exemptions are likewise pertinent within the Banking and Finance Sector in which confidentiality of savings and deposits from the customer must be maintained.

With regard to human rights, Indonesia has several regulations which are the Law No. 1 of 1946 on Indonesian Criminal Code (KUHP) (civil servants' or officials' obligation to value individuals' personal data),[19] HAM Law (human rights concept in general and the right to privacy),[20] and Law No. 21 of 2007 on Eradication of Human Trafficking (TPPO Law) (intrusion of data protection within the context of wiretapping as well as access to personal data of human trafficking suspects).[21] Moreover, in relation to telecommunication and media Indonesia has Telecommunication Law (obligation to protect the confidentiality of users' information except for wiretapping that is legally approved),[22] EIT Law (right to monitor data access towards citizen's

[17] Felicity Bell, 'Empirical Research in Law' (2016) 25 (2) Griffith Law Review' (2016) 25 Griffith 262 <http://dx.doi.org/10.1080/10383441.2016.1236440>.
[18] Aaron P Simpsons and others, 'Data Protection & Privacy – 2020'.
[19] Law No. 1 of 1946 on Indonesian Criminal Code, art 430-433.
[20] Law No. 39 of 1999 on Human Rights, art 31-32.
[21] Law No. 36 of 1999 on Eradication of Human Trafficking, art 31-32.
[22] Law No. 36 of 1999 on Telecommunication, art 40-42.

private life),[23] and Law No. 14 of 2008 on Public Information Disclosure (PID Law) (accountability in protecting personal rights through controlling the activities of public agencies).[24]

Within the scope of security and defense, data protection regime is related to Anti-Terrorism Law (authorize the access of data related to suspected parties for committing acts of terrorism),[25] Intelligence Law (wiretapping and investigation towards the flow of funds along with information in the case in which suspicious activities occur is allowed),[26] and Terrorism Funding Law (permit law enforcers to access citizens' personal data for committing terrorism). The aforementioned provisions might have a possibility of being inappropriately implemented for providing a vague limitation on the permit to personal data access.

In terms of Justice Indonesia has Law No. 8 of 1981 on Criminal Procedural Law (KUHAP) (permit violation to privacy rights as long as judicial permission is provided), Law No. 31 of 1999 on Corruption Eradication (Tipikor Law) (affirm the privacy of identities as the witness and parties of proceedings), Law No. 30 of 2002 on Corruption Eradication Commission (KPK Law (access to wiretapping and record of telecommunication is authorized for suspects or defendants), Advocate Law (protect the clients except determined by the law),[27] and JC Law (authorize access to wiretapping or recording from judge's conversation in the event where alleged violation towards judicial code of ethics occur).[28]

Concerning archives and population Indonesia has Adminduk Law (responsible for the protection of population personal data through census, etc)[29] and Archival Law (accountable for ensuring the security of personal data within state archives).[30] Furthermore, with respect to health, Medical Practice Law, Narcotics Law, Health Law, Hospital Law, Mental Health Law, and Health Workers Law. These laws are responsible for maintaining the confidentiality of patient's medical records as well as health data except required in contemplation of law enforcement.[31] Meanwhile, within Narcotics Law access towards wealth, taxation data, and wiretapping are authorized for illicit trafficking of narcotics suspects and precursors.[32]

Relating to banking and finance, the relevant regulations include Banking Law (function to decipher bank undisclosed data relating to their customers),[33] BI Law (chiefly engage in regulating banks' activities),[34] Sharia Banking Law (in the same manner function like BI Law, however it is conducted in accordance with sharia approach),[35] Money Laundering Law (have a part within citizens' right to privacy as well as averting the occurrence of money laundering),[36] and OJK Law. Undoubtedly, it can be presumed that a contradiction exists within personal data regulations examined in the aforementioned laws.

[23] Law No. 11 of 2008 on Electronic Information and Transactions, art 26(1).
[24] Law No. 14 of 2008 on Public Information Disclosure, art 6(3)(c).
[25] Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism, art 30.
[26] Law No. 17 of 2011 on State Intelligence, art 31.
[27] Law No. 18 of 2003 on Advocate, art 19.
[28] Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission, art. 20(3).
[29] Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration, art 85.
[30] Law No. 43 of 2009 on Archival, art 3(f).
[31] Law No. 29 of 2004 on Medical Practice, art 47(2); Law No. 36 of 2009 on Health, art 57; and Law No. 36 of 2014 on Health Workers, art 58(1).
[32] Law No. 35 of 2009 on Narcotics, art 75(i).
[33] Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking, art 1(28).
[34] Law No. 23 of 1999 on Bank Indonesia, art 24.
[35] ibid, art 27.
[36] Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime, art 72.

Pertinent to trade and industry, regulations in Indonesia comprise of Company Documents Law (protection within this law is provided through document retention period as well as deletion mechanism), Consumer Protection Law (as it is issued in 1999 this law is insufficient to prevent the abuse of personal data, whereas it is the main objective of this law to provide protection and to develop a further understanding regarding consumer rights in general), and Trade Law (this law does not explicitly govern about the protection of consumer's personal data, however, it is clearly stated that relevant activities within electronic system and e-commerce including trades shall refer to EIT Law as this law is legally binding).[37]

1.3. Institutions for Data Protection

There is no special institution that is fully accountable for protecting personal data in Indonesia up to now. Nonetheless, the Directorate General of Informatics Applications/Ditjen Aptika is held responsible for Indonesia's data protection regime pursuant to MoCI 20/2016.[38] Moreover, MoCI is liable for organizing governmental events that are related to communications and informatics, coordination with ESPs that include the transfer of personal data as well as requesting data and information, settling breaches of PII protection, supervision towards the enforcement of personal data protection, enforce relevant administrative sanctions towards the violation of data protection legislation, and issuing a certificate to demonstrate the worthiness of an electronic system.[39] In the case that a personal data dispute occurs, MoCI is permitted to assign Ditjen Aptika to settle the dispute and they are likewise obliged to raise public awareness relating to personal data protection.[40]

Additionally, sectoral supervision and regulatory body solely focus on the negligence towards processing activities and does not explicitly regulate about date protection. Be that as it may, several regulations examine data protection mechanisms in a diverse way, for instance, within KUHAP and EIT Law police's authorities are set under the Chairman of the District Court, while permission from the Chairman of the District Court is unnecessary under Money Laundering Law and KPK Law. Apropos to Sharia Law and BI Law, supervision towards the banking and finance sector lies within OJK's authority and that encompasses the protection of customer's personal data. Subsequently, there is no participation from foreign authorities hitherto and the Indonesian government likewise has not published the list of countries with comprehensive protection relating to transnational data transfer.

1.4. Penalties

Diverse forms of breaches among data protection laws will eventually lead to administrative sanctions, or orders and criminal penalties. The penalties shall depend on the provisions of the relevant laws and it will be limited with the sectoral competence, however, those laws will not be applicable in general although they are all associated. Moreover, individuals that collect, process, analyses, store, promote announces, transmits, or publishes personal data without legal authorization shall be condemned with administrative sanctions. It may be in a form of a verbal warning, written warning, suspension of activities, or announcement under the MoCI website for the infringement of data protection regulations.[41] Similar penalties shall be enforced in the event when there is a breach towards GR 71/2019.[42]

[37] Law No. 7 of 2014 on Trade, art 65(3).
[38] Simpson and others (n 27).
[39] ibid.
[40] ibid.
[41] Denny Rahmansyah and Farah Nabila, 'Data Protection & Cyber-security' (2019) 2 Data Protection & Cyber security 22.
[42] Simpson and others (n 27).

Breach of data protection within EIT Law in the case of unlawful access will be sanctioned with a fine of IDR 600,000,000 up to IDR 800,000,000 as well as 6-8 years of imprisonment. Within the case of alteration, addition, and reduction, IDR 2,000,000,000 up to IDR 5,000,000,000 and 8 to 10 years of imprisonment. Transmission, tampering, deletion, moving, or hiding electronic information or records will be punished with a fine of IDR 800,000,000 and 10 years of imprisonment for interception or wiretapping of a transmission.[43] Manipulation, creation, alteration, destruction, or damage of electronic information and/or documents with the aim of forging documents or other noncompliance during the processing of electronic information and/or documents shall receive a fine of IDR 10,000,000,000 to IDR 12,000,000,000 and/or 10 to 12 years of imprisonment. Additionally, violation of telecommunication law in the case of wiretapping will be imprisoned for up to 15 years. Lastly, sanctions towards several violations are regulated differently, as an illustration, criminal sanctions will be given to the violator within the Telecommunication Law and Terrorism Funding Law, while criminal sanctions along with fines will be given towards violator within Intelligence Law and KPK Law.

1.5. Enforcement

Pertinent to enforcement of the abovementioned laws, it must be highlighted that the role of the MoCI is solely to conduct an investigation subsequent to obtaining claims relating to the data subject and or ESPs and the settlement of the dispute will be handled by the Ditjen Aptika along with the relevant parties. Disputes are taken care of on a case-by-case basis due to the absence of explicit criteria towards the "loss" threshold provoked by a breach of data. Furthermore, the right to appeal towards the panel's verdict is not provided within GR 71/2019 and MoCI 20/2016. Thorough examination to obtain further understanding in settling cases relating to data protection will be done subsequently.

Under Buni Yani Case, a former lecturer from one of the private universities in Jakarta who was sentenced to 18 months in prison for editing electronic documents then made it accessible to the public and therefore violated Article 32 of the EIT Law. When the case open uproar within the public likewise appeared due to the video of the gubernatorial candidate's speech that was edited and it shows that the candidate committed the act of blasphemy. Electronic evidence was then brought to the prosecution that includes screenshots of Buni's social media account, email account, mobile phone, and the video that he uploaded on the internet.[44] Moreover, there were hacking cases that happened in 2013. One of them was sentenced to 6 months in prison with a fine for hacking into the former president's official website and the other one was sentenced to 15 months in prison for hacking the Indonesian Press Council's official website.[45]

Concerning the data transfer case, in the event of an unauthorized transfer of personal data occur the violator will be condemned with criminal sanctions. This happened to Abi Warnadi Ismentin for compiling and selling personal data without the owner's consent and hence he violated Article 32(2) of the EIT Law. Violation of this provision will receive maximum imprisonment of 9 years and or a maximum fine of IDR 3,000,000,000. It is amusing that the court managed to penalize the unauthorized access of personal data regardless of the absence of comprehensive data protection in Indonesia. Personal data was not mentioned within the provision and it only forbid unauthorized transfer of electronic information and/or documents. Nevertheless, as the personal data was transferred in an electronic form so it is contemplated as electronic information and EIT Law can be applied. It is crucial to highlight that personal data that was attained in the absence of consent can be envisaged as "unauthorized" in consonance with the EIT Law, GR 71/2019, and

[43] ibid.
[44] Rahmansyah and Nabila (n 22).
[45] ibid.

MoCI 20/2016.[46] Additionally, violation of the GR 71/2019 and MoCI 20/2016 can be settled privately in a court trial according to EIT Law and the court trial can be filed due to breach of contract or the occurrence of unlawful acts which are contrary to the laws and regulations and lead to a loss towards the plaintiff.[47]

2. The Challenges in the Enforcement of Indonesian Privacy and Data Protection Laws

2.1. Introduction

Data protection laws have a significant role within the field of data-driven economy and the implementation has become troublesome even though sufficient regulations such as the EU's GDPR exist. The problem within the enforcement lies in the regulatory, institutional, and cultural perspectives, and since Indonesia does not have uniform data protection based different challenges and issues arose.[48] The concern relating to the challenges and issues increased rapidly within the last two years. Pursuant to the initial examination, the main challenges encountered within the enforcement of the existing privacy and data protection law and regulations in Indonesia lie within regulatory, institutional, and cultural challenges. These challenges will be examined intensively within the subsequent sections.

2.2. Regulatory Challenges

There are solely 3 crucial regulations that are generally referred to within the case of personal data protection in Indonesia, besides the fact that the existing data protection regime is separated within 30 regulations. They are the EIT Law, GR 71/2019, and MoCI 20/2016. However, the enforcement of the data protection regime is not limited to these laws, and the other regulations shall be applied when necessary. To provide a coherent understanding of the aforementioned regulations it is pertinent to note that there are several limitations within those regulations. Article 26(1) of the EIT Law regulates within the scope of processing, transmission, and sharing/transfer of personal data through an electronic system and it is applicable for individuals as well as companies. Article 1(29) of the GR 71/2019 is limited to the collection, management, and processing of personal data within electronic and non-electronic systems and applies to individuals, state institutions, and companies. In addition, Article 1(1) and 1(2) of MoCI 20/2016 focuses on the scope of acquisition, collection, processing, storage, display, announcement, transfer, sharing, and annihilation of personal data within electronic systems and are applicable individual, state institutions, business entities, or civil society that operate and/or utilize electronic systems.

According to the abovementioned elaboration, the utilization and transfer of personal data without an individual's consent are prohibited under Article 26 of the EIT Law. In the event when this happens, individuals are authorized to file a claim and receiving financial compensation and ESPs are accountable for revoking irrelevant electronic information or documents through a court decision. This law does not provide a clear-cut interpretation of personal data. ESPs' responsibilities that involve notifying users of personal data failure are stipulated under GR 82/2012 (amended by GR 71/2019). Identical to EIT Law, coherent explanation and scope of personal data is not specified and result in the difficulties of accessing data processing operations. Contrary to the abovementioned laws, clearer personal data definition, as well as the subjects' rights,[49] are laid down within the MoCI 20/2016 and it incorporates the concern of personal data itself along with the types of personal data. In a nutshell, the aforementioned regulations solely address personal data handled through electronic systems, while non-electronic systems are imposed under sectoral regulation specified above.

[46] K&K Advocates, 'Unauthorized Transfer of Personal Data Might Be Punishable Under the Indonesian Criminal Law'.
[47] ibid.
[48] Putri (n 1).
[49] MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems, art 26.

Afterward, limitations of 5 years minimum are set forth towards the retention period of personal data under the MoCI 20/2016. Archiving, retention data, and personal data within government institutions are stipulated under Archival Law, while the retention period in the business sector is regulated individually. Despite MoCI 20/2016 details on personal data protection, it is not sufficient enough for significant enforcement, at the same time EIT Law does not provide a coherent definition of personal data but has strong sanctions.[50] The government is complying with sectoral regulations instead of the MoCI 20/2016 and business sectors are referring to the GDPR and PDPA in advancing their data protection policies, hence, expecting comprehensive enforcement is harder.[51] In conformity to the thorough elaboration above, regulatory challenges are apparent from the inadequacy of the current data protection regulation. To provide a substantial illustration, current regulation solely focuses on ESPs' obligation in collecting, processing, and using personal data regardless of its lack of details within data subjects' rights and the ones who are accountable to protect these rights.

2.3. Institutional Challenges and Accountability Process

Primary institutional challenges within the government of Indonesia throughout the implementation of the existing data protection regime consisting of overlapping responsibilities and a lack of knowledge, capacities, and capabilities of regulators.[52] First and foremost, with regard to overlapping responsibilities, there is an absence of a data protection authority that is accountable to supervise the protection of personal data. Related disputes are still handled by ministries or independent agencies that are responsible within the relevant fields, to provide a clearer picture, Ditjen Aptika is responsible for settling personal data disputes carried out by ESPs, OJK is accountable for breaches within the financial sector, and Ministry of Health is in charge for breaches relating to any issues in the health sectors. In relation to the second challenge, it is undeniable that a great deal of state officials are unaware of the fact that they are processing people's personal data as specific regulation does not exist and the existing regulations essentially focus on ESPs, therefore, the realization of being bound to the regulations is missing. This is contrary to the stipulation of MoCI 20/2016 that explicitly defines the relevancy of this regulation to state officials that are in charge of processing personal data within the electronic system.

By the same token, MoCI aspires to enhance state officials' competencies and knowledge by way of encouraging capacity-building programs relating to data protection in a form of sending state officials to join workshops, training, and certification programs. As in the business sector, they have greater institutional capacities because they have designated officers under the Legal and Compliance Department or IT Department that is responsible for handling personal data protection issues.[53] Guidelines for personal data protection to comply and enforce the existing regulation like the Indonesian Fintech Lender Association (AFPI) have likewise been created by business associations.[54]

In addition, institutional challenges likewise include accountability issues for the reason that sanctions given are weak, an independent investigator is unavailable, and overlapping authorities in dealing with misuse of personal data which generally obtained by the MoCI with no permit to enforce sanctions and solely function as an intermediary. MoCI commonly transfers cases to the Attorney Office of Indonesia or another relevant sectoral ministry like OJK. The World Wide Web

[50] Graham Greenleaf, 'Global Tales of Data Privacy Laws and Bills (5th Ed 2017, Updated March 2017)' [2017] Privacy Laws & Business International Report.
[51] Putri (n 1).
[52] ibid.
[53] ibid.
[54] ibid.

Foundation, human rights organizations, state officials, and representatives from the business sector acknowledge that inadequate proof in processing lawsuits relating to misuse of personal data.[55] Aside from the abovementioned explanation, a specific procedure in ensuring transparency as well as accountability within a data protection regime does not exist.[56]

2.4. Social and Cultural Challenges

With regard to the absence of a sufficient data protection regulation, Indonesian citizens are considered as the most susceptible parties as their awareness relating to this matter is relatively low and it is not deliberately guarded. This issue is highly correlated with the cultural background which is a pertinent aspect within the regulatory privacy mechanism and according to this verifiable truth, the cultural characteristics within the drafting and enforcement of the relevant regulations have not been considered by Indonesia. Discussion relating to privacy and personal data is pretty difficult to conduct as it is distinguished as a security rather than a human right and the fear of returning to the era in which everything was protected by the government exists. Moreover, most citizens disregard privacy risks and personal data misuse for online free services, applications, or loan providers.[57]

Notwithstanding the number of cases that occur in Indonesia relating to privacy and personal data turns out that the awareness towards these issues is close to the ground. Therefore the government must carry out its responsibility to provide sufficient protection as well as enhance the awareness to Indonesian citizens regarding this issue. It is likewise important to educate the citizens about the value of securing their personal data.[58] Furthermore, the draft of the Indonesian data protection regulation is referring to GDPR for its most remarkable competency. Nevertheless, GDPR cannot be referred to all the time because European citizens understanding of the concept of data protection is dissimilar to Indonesian citizens as the concept of data protection has been implanted to the European citizens since 1995 and subsequent to the enforcement of the law in 2018 the EU has implemented a huge effort by attributing EUR 5 million to 19 projects with the aim of spreading awareness relating to this issue.[59] Contrary to the EU, establishing a sufficient legal framework regarding personal data protection, sustaining the growing digital economy, and educating citizens is still troublesome for Indonesia.[60] On that account, referring to neighboring countries' data protection regulations like the Philippines and Singapore shall be beneficial for Indonesia taking into account the similarities within the income level and industrialization in Indonesia.[61]

2.5. Recommendations and Measures That Can Be Adopted by Indonesian Government

Despite the fact that a unified regulation concerning personal data protection does not exist, however, the right to privacy is protected but not enforced properly under Article 28(G)(1) of the Indonesian Constitution and affirm under Article 29 of HAM Law. Hence, the case in which the right to privacy or personal data is neglected can be found easily.[62] In response to the extensive data collection towards diverse forms of data towards certain interests, the Indonesian government has the urgency to establish tenacious regulations for the citizens. Therefore, prevailing to the

[55] ibid.
[56] ibid.
[57] Kharishar Kahfi, 'Concern Grows over Data Protection at Online Loan Services' (*The Jakarta Post,* 6 July 2018) < https://www.thejakartapost.com/news/2018/07/06/concern-grows-over-data-protection-online-loan-services.html>.
[58] Putri (n 1).
[59] Sabine Trepte and others, 'A Cross-Cultural Perspective on the Privacy Calculus' (2017) 3 Social Media and Society.
[60] Putri (n 1).
[61] ibid.
[62] Djafar (n 2).

examination several recommendations and measures ought to be taken into consideration by the Indonesian government and it will be elaborated afterward.[63]

To begin with, providing clear guidelines towards data collection and processing shall be the most essential approach instead of enacting rigid regulations in consideration of Indonesian citizens' lack of understanding concerning privacy and data protection. This approach ought to be applied within government institutions, companies, etc. Although this will not be sufficient enough and thorough examination must be implemented. On the other hand, a single-independent body/agency that is strictly controlled by relevant stakeholders, transparent, and accountable for data protection must be provided considering the inherent work within government institutions along with collections and processing of personal data. The body/agency, functionality, structure, and state budget must be carefully considered and suggestion from parliament relating to this independent agency as regulation pillars can likewise be a good alternative.[64]

Supplementary to the aforesaid recommendations, gradation on financial penalties conforming to the legal subject, size of enterprise, company, or organization, and/or personal data quantity that is processed shall be necessary for the event when administrative sanctions are falling short.[65] Furthermore, regulatory sandbox model that is enhanced along with the advancement of business models and innovation that may as well be a form of assimilation towards the enforcement of the existing law and formation of the upcoming law while cultivating the advancement of an avant-garde digital ecosystem ought to be enforced as it functions to handle two primary concerns simultaneously that include the development of digital innovations and uncertainty within the existing law itself.[66] Finally yet importantly, Indonesian citizens' development within the privacy and personal data proficiency must be strengthened and harmonized to advance the cultural dimension within the enforcement of data protection regulation. This likewise will settle the gap of privacy culture and knowledge within Indonesian citizens along with assisting Indonesian citizens in enhancing their cultural sensitivity relating to privacy and personal data.

3. Key Elements to Be Taken Into Account by the Indonesian Policymakers in Regard to the Need of a Unified Privacy and Data Protection Law

3.1. Introduction

Legal framework, objectives, goals, notable provisions, data protection institutions, penalties, and enforcement that functions as the protection of personal data in the EU and Singapore shall be examined meticulously within this section. Both regulations will be deliberated and preferred to assist policymakers in Indonesia to establish comprehensive regulation in consideration of the deficiency within Indonesian data protection regulations that were elaborated previously.

3.2. The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

The earliest personal data protection law in the EU was enacted in 1995 by the Data Protection Directive 95/46/EC (1995 Directive) and it was converted into diverse national laws because it was not enforced directly. Until the following 20 years advanced GDPR that include additional elements relating to the approach, rights, and obligations applicable for the Member States as a law aiming to harmonize data protection law was enacted. There are 3 main objectives of GDPR,[67] first off to harmonize data protection laws in the EU without transposing GDPR into the national

[63] ibid.
[64] ibid.
[65] Putri (n 1).
[66] Elizabeth Denham, 'Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice'1; Putri (n 1).
[67] The European Union Regulation 2016/679 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of Such Data (GDPR), art 1.

and regulatory framework,[68] GDPR demand the protection of primary rights by way of protecting individual's rights relating to personal data as well as constituting primary rules to safeguard any activities relating to individuals' personal data,[69] and securing the flexibility of data as European internal market obligate free movement of data and it is represented under the economic rationale of the law.[70]

The main principles of data protection as imposed under the GDPR that formulates the preceding objectives comprise of lawfulness, fairness, and transparency, the purpose of limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, and accountability.[71] Aside from these principles, the legitimacy of data processing can solely be conducted by fulfilling several requirements involving consent from the data subject, when the data subject is the party of the performance of a contract or about to enter a contract, when the subject is complying with a legal obligation, relating to the protection of data subject or natural person, function as public interest or legitimate interest controlled by third party nor controller except the interest surpassed the primary rights and freedom of data subject especially when it is a child.[72] Additionally, consent will construct safer online data processing environment[73] and it must be administered in a clear affirmative act according to Article 7 of the GDPR that lays down a great verge in protecting individuals' personal data.[74]

Pursuant to the aforesaid key provisions from GDPR it can be concluded that careful evaluation procedures of data processing, vet service providers, and contractual limits towards data use must be implemented by companies, a high standard on lawful consent is set by GDPR, and companies are invigorated by GDPR to enhance information governance frameworks, in-house data use, ensuring that humans will not be left behind during decision making,[75] and in general, it has a higher standard, stricter, as well as tougher sanctions, compared to the 1995 Directive. Data Protection Authorities/Supervisory Authority (DPA) that functions to ensure citizens' personal data with its investigative, corrective, authorization, and advisory authority currently exist and is regulated under the GDPR.[76] On-site data protection audits, issuing questionnaires, public warnings, reprimands, as well as imposing sanctions and fines can likewise be done by the DPA.[77] Meanwhile, the central data protection authority rest under the European Data Protection Board (EDPB) with its obligation to monitor, supervise, settling issues that occur among national DPA's, and providing guidance to DPA.[78]

Furthermore, fines as an additional penalty or replacement towards further remedies/corrective powers that are imposed to the violations of data protection within GDPR are determined by DPAs. Breaches towards basic principles for data processing and consent, data subjects' rights, international transfer restrictions, obligations imposed by member state law like employee data processing, and DPA's orders will be sentenced with up to EUR 20 million or 4% of the total worldwide turnover of the preceding year.[79] As for breaches towards controllers and processors'

[68] ibid, art 1(1); Treaty of Functioning of the European Union (TFEU), Consolidated Versions of TFEU 2012/C326/01, art 288.
[69] Article 1(2) of the GDPR; Article 2 of the GDPR Recital.
[70] Article 1(3) of the GDPR; Recital 2, 6, 7, & 13 of the GDPR.
[71] Article 5(1) & (2) of the GDPR.
[72] ibid, art 6(1).
[73] Neil Robinson and others, 'Review of the European Data Protection Directive' [2009] RETR 1.
[74] Article 1(11) in conjunction with Recital 32 of the GDPR.
[75] Article 7 of the GDPR; Hoofnagle, Sloot, and Borgesius (n 17).
[76] The Charter of Fundamental Rights of the European Union 2012/C 326/02 (the Charter), art 8(3); Article 57 & 58 of the GDPR.
[77] DLA Piper, 'Data Protection Laws of the World – Full Handbook'.
[78] Crowell and Moring, 'The New European General Data Protection Regulation'.
[79] Article 83(5) of the GDPR.

obligations, security and data breach notification obligations, certification bodies' obligation, and monitoring bodies' obligations will be punished with a fine up to EUR 10 million or 2% of the total worldwide turnover of the preceding year.[80]

281,088 cases in which 144,376 related to consumer complaints and 89,271 related to data breach notifications by data controllers logged by various DPA's throughout the year since GDPR came into force have already taken place.[81] Nevertheless, there were only 91 GDPR fines handed out in the European Economic Area within the first 8 months since GDPR came into force.[82] Moreover, the numbers have developed according to EDPB's report in February 2019 proving that 11 countries had implemented GDPR fines with a total amount of around EUR 56 million.[83] In the same manner, GDPR awareness was facilitated sufficiently by the Dutch DPA by equipping information, guidelines, and tools about its website's regulation. As an illustration, violation towards data subject rights for charging fees and discouraging individuals in need of their personal data access conducted by the Dutch Credit Registration Bureau (BKR) was sentenced by the Dutch DPA with a fine of EUR 830,000.[84] In contrast, DPA's are regulated under state level in Germany that results in 16 data regulators and has conjointly released 75 fines following the enactment of GDPR with the total of EUR 449,000 with the largest fine of EUR 80,000 with regard to the violation towards personal data within the healthcare organization. On the other hand, the 2 largest violations towards the enactment of GDPR relating to data breach-related violations derived from the UK's Information Commissioner's Office in which British Airways was sentenced with a fine of GBP 183.4 million and GBP 99.2 million in the case of Marriot.[85]

3.3. The Personal Data Protection Act 2012 (PDPA) (Regulation No. 26 of 2012)

PDPA is a crucial aspect within Singapore's technology law framework subsequent to the enactment on 20th November 2012 and enforcement on 2nd July 2014.[86] Singapore was previously similar to Indonesia relating to the data protection regulations as sectoral regulations were likewise imposed previously[87] and it was enhanced from the influence of data protection regimes of the EU, UK, Canada, Hong Kong, Australia, New Zealand, the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data as well as the APEC Privacy Framework.[88] Individual personal data under PDPA is stipulated by organizations in which both right of individuals in protecting their personal data and the need of organizations to collect, use, and disclose personal data in an appropriate situation and these provisions cover data protection and the DNC registry.[89]

---

[80] ibid, art 83(4).
[81] Neil Hodge, 'GDPR Enforcement Varies Widely by County' (*Compliance Week,* 2019) <https://www.complianceweek.com/gdpr/gdpr-enforcement-varies-widely-by-country/27436.article> accessed 13 February 2020.
[82] ibid.
[83] DLA Piper, 'DLA Piper GDPR Data Breach Survey: February 2019'.
[84] Joke Bodewits and Benjamino Blok, 'Dutch DPA Issues Record Fine For Violating GDPR Data Subject Rights' (*Engage.hoganlovells.com*, 2020). See <https://www.engage.hoganlovells.com/knowledgeservices/news/dutch-dpa-issues-record-fine-for-violating-gdpr-data-subject-rights#:~:text=Dutch%20DPA%20issues%20record%20fine%20for%20violating%20GDPR%20data%20subject%20rights,-7%20July%202020&text=The%20Dutch%20Data%20Protection%20Authority,for%20violating%20data%20subject%20rights.> accessed 26 October 2020.
[85] Hodge (n 125).
[86] Personal Data Protection Act 2012 (Act No. 26 of 2012) (PDPA).
[87] Section 4(6)(b) of the PDPA.
[88] Personal Data Protection Commission - Singapore, 'PDPA Overview' (*pdpc.gov.sg*) <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act> accessed 25 August 2020.
[89] Personal Data Protection Commission – Singapore (n 19).

Moreover, PDPA has 3 main objectives that include giving an individual right to data, recognize the qualified right of private organizations in collecting, using, and disclosing personal data, and ensuring that Singapore has equal data protection laws to facilitate cross-border data transfers. In terms of content, PDPA is quite similar to the key provision of GDPR explicitly under Article 5.

The legal basis for the data processing is clearly defined under Article 6 of GDPR, unlike PDPA. Under Section 13 of the PDPA, collection, use, or disclosure of personal can solely be done with the consent of the individual.[90] The enforcement of PDPA has the aim of showing the sufficiency of the administration and the sanctions of PDPA. PDPA is under the supervision of the Personal Data Protection Commission (PDPC) of Singapore with the authorities to investigate powers, provides guidance and auditing services, issues guidelines and advisories, and is responsible to spread awareness relating to data protection and privacy.[91]

Pertinent to the violation of PDPA, the amount of fine/prison is determined based on the relevant provisions. A maximum fine of SGD 5,000 and/or maximum imprisonment of 12 months will be implemented in the event when unauthorized access or unlawful modification towards citizens' personal data occur.[92] Fine up to SGD 100,000 will be enforced on organizations and a fine up to SGD 10,000 or imprisonment will be imposed on individuals if breaches of PDPC occur while performing their responsibilities and enforcing their authorities.[93]

Furthermore, disputes relating to private matters can be settled by a civil lawsuit.[94] Per June 2019, 90 orders against 114 organizations breached the PDPA and it is due to the mediocre security arrangements, failure within the mass email and/or post, and internal data protection policies that are inadequate.[95] Up to now, the highest fines imposed by PDPC towards organizations are SGD 250,000 and SGD 750,000 pro-rata to SingHealth Services Pte Ltd for data breach due to cyber-attack on patients' database system and Integrated Health Information Systems Pte Ltd.[96] PDPC likewise implemented a mix of behavioral remedies with financial penalties.

Moreover, a fine of SGD 20,000 was imposed by the PDPC in December 2018 towards WTS Automotive Services Pte Ltd for a failure within security arrangements. Another identical case appears in the first half of 2019 in which a fine of SGD 16,000 was enforced to GrabCar Pte Ltd. Within the same period a fine of SGD 8,000 was laid down to Matthew Chiong Partnership for failure to fulfill transparency obligation.[97]

As a comparison, it can be seen that significant differences between the GDPR and the PDPA lie within the enforcement of monetary penalties within cases of regulations' non-compliance and the GDPR's maximum limit towards monetary penalties are relatively higher than the PDPA. Pursuant to the aforementioned examination, DPAs developed guidelines to calculate the number of monetary penalties, while PDPA does not have identical policies like the GDPR. Nevertheless, within PDPC's guide on Active Enforcement, financial penalties are solely applicable for serious

[90] Section 13 of the PDPA.
[91] Chong Kin Lim and Janice Lee, 'Singapore - Data Protection Overview' (*DataGuidance*, 2019) <https://www.dataguidance.com/notes/singapore-data-protection-overview> accessed 8 September 2020.
[92] Section 51(2) of the PDPA.
[93] Warren B Chik, 'The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy' (2013) 29 Computer Law and Security Review 554.
[94] Section 32 of the PDPA.
[95] Part X of the PDPA.
[96] See Re Singapore Health Services Pte Ltd and another [2019] SGPDPC 3.
[97] Yuet Ming Tham, 'Singapore - The Privacy, Data Protection And Cyber-security Law Review - Edition 6 - TLR - The Law Reviews' (*Thelawreviews.co.uk*, 2019) <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210086/singapore> accessed 8 September 2020.

breaches.[98] The limitation within this guide may lead to a discrepancy towards the number of fines enforced by the GDPR and the PDPA. Another crucial aspect that must be highlighted is that PDPA is stipulated solely for commercial and economic development not for the government, unlike the GDPR that is enacted for both government and public.

3.4. Lesson That Can Be Learned From the EU and Singapore

Conforming to the thorough elaboration towards the GDPR and the PDPA it is clear that both regulations are sufficient to protect data subjects and it is in light of the fact that efficient sanctions are imposed within both regulations. Hence, companies' activities are bound to comply with both regulations and it is pertinent for Indonesian policymakers to refer to several crucial elements within the GDPR and the PDPA as both regulations are contemplated to be sufficient from both mechanism and frameworks especially with their comprehensive concepts and principles.

The first lesson that shall be considered from the aforesaid regulations is harmonization towards the existing Indonesian regulations. As mentioned previously, the EU managed to harmonize the data protection laws from various EU member states into GDPR that is applied directly to all member states. Unlike the EU or the United States of America, Indonesia is not a union in which laws and regulations will be applied nationally and directly towards all Indonesian citizens. According to the abovementioned examination as Indonesian regulations on data protection are contemplated as insufficient and overlapping,[99] Indonesian policymakers must adopt the EU's regulatory harmonization concept relating to data protection regulation as overlapping should not be an issue as long as it can be implemented comprehensively without causing any confusion throughout the enforcement. In this case, Indonesian policymakers shall establish a new regulation that covers all aspects of Indonesia's data protection activities including data processing activities and it must be specified under a unified and comprehensive framework. Instead of eliminating the existing principal and sectoral regulations, it ought to be strengthened to create comprehensive data protection regulations that will likewise solve the currently existing problems which are the overlapping and inadequateness of the current sectoral regulations.

Subsequently, another essential lesson that must be taken into consideration is a mandatory designation of data protection authority. In line with the prior examination, it is proven that the designated national data protection authority that is specifically accountable for data protection in Indonesia does not exist. There is only the MoCI by way of Ditjen Aptika, however, they cannot be contemplated as Indonesia's designated data protection authority for the reason that supervising the protection of personal data is not their fundamental responsibility.[100] Moreover, having a designated data protection authority will guarantee the safety of personal data efficiently.

Relating to the increase of data protection breaches, many disputes were not settled through court proceedings, as an illustration, within cases of online lending service providers, they were solely punished through the cancellation of their license by OJK. Contrary to the activities of EU's DPA and Singapore's PDPC, as a designated institution they were mandated with a solid authority to supervise the protection of personal data within their jurisdiction that results in a greater imposition of the GDPR and PDPA. In addition, MoCI and Ditjen Aptika were not created for the sake of safeguarding Indonesian data protection that leads to the insufficient and weak imposition of laws. Thus, constructing a designated national data protection authority similar to the PDPA and PDPC authorities will assist the Indonesian data protection regime in reducing data protection issues.

---

[98] Angela Potter and others, 'GDPR v. Singapore's PDPA Comparing Privacy Laws:' Comparing Privacy Laws: GDPR v. Singapore's PDPA.

[99] Djafar (n 2).

[100] 'Functions of Ministry of Communications And Informatics' (*Website of Ministry of Communications and Informatics*) <https://www.kominfo.go.id/tugas-dan-fungsi> accessed 16 September 2020.

The next lesson in line that must be adopted by Indonesia is the designation of data protection officer. Looking right into the EU's practice, Data Protection Officer (DPO) is pointed by member states in ensuring conformity with the GDPR. DPOs responsibilities are explicitly set forth under Article 29 of the GDPR that basically function to inform and advise organizations where DPOs work, monitor compliance, conduct data protection impact assessment (DIPA), and as a mediator within the national data protection authority.[101]

This concept is likewise present in Singapore where DPO keep track of data protection responsibilities and guarantee the conformity with the PDPA.[102] Therefore, Indonesia policymakers must take up the EU and Singapore DPO obligation mechanism for the new data protection law to increase compliance, at the very least from organizations' side as they are responsible for establishing organizations' data protection strategy as well as practical implementation and that means personal data users are obliged to recruit DPO to their organizations as it will beneficial for the organizations because DPO will supervise and assure that they obey the law in processing personal data, it will likewise enhance organizations' way in terms of protecting and controlling personal data while data processing activities are carried out, and ensure the consistency of data processing activities with the relevant data protection law.[103] Conjointly, DPO can be the primary contact relating to the request of personal data matters,[104] they can function as the extension of governmental authority.[105]

Last but not least, with regard to the do-not-call registry provision. PDPA essentially balances both individuals' right to their personal data and the organization's need to collect, use, or disclose personal for a legitimate purpose. Furthermore, relating to the DNC provision that regulates specific marketing messages to Singaporean telephone numbers and maintained by section 39 of the PDPA, they are accountable to check relevant DNC registers, provide information for individuals or organizations with the authorization to send marketing messages, and make sure that calling line identity is transparent.[106] Relevant to this matter, Indonesia is acknowledged as the third-most spammed country in the world according to Truecaller Insights Report 2019 in which Indonesian citizens obtain up to 27.9 spam nonconsensual calls monthly for marketing purposes with 40% from financial services and 23% from insurance brokers as the country's top spammers.[107] This might be prohibited implicitly by the OJK through Regulation No. 1/2013, nevertheless, other regulations relating to advertising and marketing do not exist and solely depends on the general requirement for obtaining data subject consent. On that account, Indonesian policymakers must take up and grasp the DNC provisions as a reference for the upcoming data protection legal framework.

---

[101] Article 39(1) of the GDPR.

[102] 'Personal Data Protection Commission - Singapore, Data Protection Officers' (*pdpc.gov.sg*) <https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers#:~:text=In%20particular%2C%20organisations%20are%20required,of%20developments%20in%20the%20PDPA.> accessed 16 September 2020.

[103] Christoph Klug, 'Improving Self-Regulation through (Law-Based) Corporate Data Protection Officials' [2002] Privacy Laws & Business International Newsletter 1.

[104] Muhammad Iqsan Sirie, 'The Mandatory Designation of a Data Protection Officer in Indonesia's Upcoming Personal Data Protection Law' (2018) 5 PADJADJARAN Jurnal Ilmu Hukum (Journal of Law) 24 <http://jurnal.unpad.ac.id/pjih/article/view/13991>.

[105] ibid.

[106] Russel Butarbutar, 'Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia' (2020) 130 Advances in Economics, Business and Management Research 154.

[107] 'Indonesia named third-most Spammed Country in the World' (*The Jakarta* Post*,* 7 December 2019) <https://www.thejakartapost.com/life/2019/12/07/indonesia-named-third-most-spammed-country-in-the-world.html>; Kim Fai Kok, 'Truecaller Insights: Top 20 Countries Affected by Spam Calls & SMS in 2019' (*Truecaller,* 3 December 2019) <https://truecaller.blog/2019/12/03/truecaller-insights-top-20-countries-affected-by-spam-calls-sms-in-2019/>.

CONCLUSION

At a later date, Indonesia has a high potential of having a vigorous digital economy, however, challenges in terms of weak quality services, uneven digitization, and unregulated digital infrastructure hinder its way to unlock the potential. This potential arises from the growth of digital consumers that are relatively high and due to the occurrence of the Covid-19 crisis, the national e-commerce policy (GR 80/2019) plays an important role in advancing the country's infrastructure. These steps towards digitization ensure higher standards with regard to the citizen's data protection. However, Indonesia's data protection regulation deals with a bunch of obstacles. Addressing these challenges are the main objectives of this thesis. Examination of the approach of settling data protection issues and the nature of penalties imposed under Indonesian regulations are likewise imposed.

Besides the deficiency among regulatory and institutional aspects, Indonesia likewise encounters unique cultural problems in which privacy and personal data security are not contemplated as an inherent part of life despite knowing their data being enormously traded. This is contrary to the issue encountered by the EU and Singapore relating to spreading awareness to the citizens in ensuring their knowledge towards the importance of data protection in order to be sufficiently circulated to the public. Moreover, apart from thorough examination concerning these challenges, suggestions that must be adopted by Indonesian policymakers are likewise discussed by comparative analysis towards the EU and Singapore data protection framework for the upcoming data protection regulation. The in-depth analysis resulted in 4 primary suggestions that comprise the importance of harmonization among current Indonesian sectoral regulations that are presumed to be insufficient and overlapping, the need of designated DPA by adopting the DPA concepts from the GDPR and the PDPA as well as DPO for the compliance towards the upcoming data protection regulation, and the urgency to adopt the value of DNC provision from PDPA relating to spam messages. Lastly, as the Indonesian government suggested to complete the proposed personal data protection bill, a stronger endeavor towards citizens' concern is expected and the currently existing issues relating to data protection law in Indonesia can be ultimately settled to assist the country in realizing its impressive potential within the digital economy.

ACKNOWLEDGMENT

This article is based on the Master of Laws thesis the author submitted for the Master Program in Law and Technology in Tilburg Law School (*Universiteit van Tilburg*).

REFERENCES

Statures and Statutory Instruments

Charter of Fundamental Rights of the European Union 2012/C 326/02 (the Charter).

General Data Protection Regulation (Regulation (EU) 2016/679).

Indonesian Law No. 1 of 1946 on Criminal Code.

Indonesian Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism.

Indonesian Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking.

Indonesian Law No. 11 of 2008 on Electronic Information and Transactions.

Indonesian Law No. 14 of 2008 on Public Information Disclosure.

Indonesian Law No. 17 of 2011 on State Intelligence.

Indonesian Law No. 18 of 2003 on Advocate.

Indonesian Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission.

Indonesian Law No. 23 of 1999 on Bank Indonesia.

Indonesian Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration.

Indonesian Law No. 29 of 2004 on Medical Practice.

Indonesian Law No. 35 of 2009 on Narcotics.

Indonesian Law No. 36 of 1999 on Eradication of Human Trafficking.

Indonesian Law No. 36 of 1999 on Telecommunication.

Indonesian Law No. 36 of 2009 on Health.

Indonesian Law No. 36 of 2014 on Health Workers.

Indonesian Law No. 39 of 1999 on Human Rights.

Indonesian Law No. 43 of 2009 on Archival.

Indonesian Law No. 7 of 2014 on Trade

Indonesian Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.

MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems.

Singapore Personal Data Protection Act 2012 (Act No. 26 of 2012) (PDPA).

Case Laws

Re Singapore Health Services Pte Ltd and another [2019] SGPDPC 3.

Journal Articles

Butarbutar R, 'Initiating New Regulations on Personal Data Protection: Challenges for Personal Data Protection in Indonesia' (2020) 130 Advances in Economics, Business and Management Research 154.

Chik W, 'The Singapore Personal Data Protection Act and an Assessment of Future Trends in Data Privacy' (2013) 29 Computer Law and Security Review 554.

Crowell &Moring, 'The New European General Data Protection Regulation'.

Denham E, 'Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice' 1.

Djafar W, 'Big Data Dan Pengumpulan Data Skala Besar Di Indonesia: Pengantar Untuk Memahami Tantangan Aktual Perlindungan Hak Atas Privasi'.

Djafar W, Sumigar B and Setianti B, 'Perlindungan Data Pribadi - Usulan Pelembagaan Kebijakan Dari Perspektif Hak Asasi Manusia' [2016] Seri Internet dan Hak Asasi Manusia.

DLA Piper, 'Data Protection Laws of the World – Full Handbook'.

DLA Piper, 'DLA Piper GDPR Data Breach Survey: February 2019'.

Greenleaf G, 'Global Tables of Data Privacy Laws and Bills (5th Ed 2017, Updated March 2017)' [2017] Privacy Laws & Business International Report.

Hutchinson T, 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law' (2016) 38 Erasmus Law Review.

K&K Advocates, 'Unauthorized Transfer of Personal Data Might Be Punishable Under the Indonesian Criminal Law'.

Klug C, 'Improving Self-Regulation through (Law-Based) Corporate Data Protection Officials' [2002] Privacy Laws & Business International Newsletter 1.

Personal Data Protection Commission – Singapore, 'Advisory Guidelines on Key Concepts in the Personal Data Protection Act'.

Potter A and others, 'GDPR v. Singapore's PDPA Comparing Privacy Laws:' Comparing Privacy Laws: GDPR v. Singapore's PDPA.

Putri D, 'Personal Data Protection in Indonesia: The Long Road to Effective Implementation' [2019] World Wide Web Foundation.

Rahmansyah D and Nabila F, 'Data Protection & Cyber-security' (2019) 2 Data Protection & Cyber-security 22.

Robinson N and others, 'Review of the European Data Protection Directive' [2009] Rand Europe Technical Report 1.

Rosadi S, 'Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia' (2018) 5 Brawijaya Law Journal 143.

Rosadi S, 'Protecting Privacy on Personal Data in Digital Economic Era: Legal Framework in Indonesia' (2019).

Simpsons AP and others, 'Data Protection & Privacy – 2020'.

Trepte S and others, 'A Cross-Cultural Perspective on the Privacy Calculus' (2017) 3 Social Media and Society.

Online Journals

Bell F, 'Empirical Research in Law' (2016) 25 (2) Griffith Law Review' (2016) 25 Griffith 262 <http://dx.doi.org/10.1080/10383441.2016.1236440>.

Bodewits J and Blok B, 'Dutch DPA Issues Record Fine For Violating GDPR Data Subject Rights' (*Engage.hoganlovells.com*, 2020) <https://www.engage.hoganlovells.com/knowledgeservices/news/dutch-dpa-issues-record-fine-for-violating-gdpr-data-subject-rights#:~:text=Dutch%20DPA%20issues%20record%20fine%20for%20violating%20GDPR%20data%20subject%20rights,-7%20July%202020&text=The%20Dutch%20Data%20Protection%20Authority,for%20violating%20data%20subject%20rights>.

Hodge N, 'GDPR Enforcement Varies Widely by Country' (*Compliance Week*, 2019) <https://www.complianceweek.com/gdpr/gdpr-enforcement-varies-widely-by-country/27436.article> accessed 13 February 2020.

Hoofnagle C, Sloot B and Borgesius F, 'The European Union General Data Protection Regulation: What It Is and What It Means' (2019) 28 Information & Communications Technology Law 65 <https://doi.org/10.1080/13600834.2019.1573501>.

Sirie M, 'The Mandatory Designation of a Data Protection Officer in Indonesia's Upcoming Personal Data Protection Law' (2018) 5 PADJADJARAN Jurnal Ilmu Hukum (Journal of Law) 24 <http://jurnal.unpad.ac.id/pjih/article/view/13991>.

Websites and Articles

'Indonesia named third-most Spammed Country in the World' (*The Jakarta* Post*,* 7 December 2019) <https://www.thejakartapost.com/life/2019/12/07/indonesia-named-third-most-spammed-country-in-the-world.html>.

'Functions of Ministry of Communications And Informatics' (*Website of Ministry of Communications and Informatics*) <https://www.kominfo.go.id/tugas-dan-fungsi> accessed 16 September 2020.

Kahfi K, 'Concern Grows over Data Protection at Online Loan Services' (*The Jakarta Post,* 6 July 2018) < https://www.thejakartapost.com/news/2018/07/06/concern-grows-over-data-protection-online-loan-services.html>.

Kok K, 'Truecaller Insights: Top 20 Countries Affected by Spam Calls & SMS in 2019' (*Truecaller,* 3 December 2019) <https://truecaller.blog/2019/12/03/truecaller-insights-top-20-countries-affected-by-spam-calls-sms-in-2019/>.

Lim C and Lee J, 'Singapore - Data Protection Overview' (*DataGuidance*, 2019) <https://www.dataguidance.com/notes/singapore-data-protection-overview> accessed 8 September 2020.

'Personal Data Protection Commission - Singapore, Data Protection Officers' (*pdpc.gov.sg*) <https://www.pdpc.gov.sg/overview-of-pdpa/data-protection/business-owner/data-protection-officers#:~:text=In%20particular%2C%20organisations%20are%20required,of%20developments%20in%20the%20PDPA.> accessed 16 September 2020.

Personal Data Protection Commission - Singapore, 'PDPA Overview' (*pdpc.gov.sg*) <https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act> accessed 25 August 2020.

Tham Y, 'Singapore - The Privacy, Data Protection And Cyber-security Law Review - Edition 6 - TLR - The Law Reviews' (*Thelawreviews.co.uk*, 2019) <https://thelawreviews.co.uk/edition/the-privacy-data-protection-and-cybersecurity-law-review-edition-6/1210086/singapore> accessed 8 September 2020.

Official Documents

Otoritas Jasa Keuangan (Financial Services Authority), 'Otoritas Jasa Keuangan dan BARESKRIM POLRI Sepakat Berantas Fintech Peer-To-Peer-Lending Ilegal dan Investasi Ilegal'.