PRIVACY AND DATA PROTECTION: INDONESIAN LEGAL FRAMEWORK

“It is never too late to realize that Data is the new Prada!”

Thesis of Master Program in Law and Technology
Tilburg Law School
Universiteit van Tilburg

Written by:
Brahmantyo Suryo Satwiko
SNR: 2037895 - ANR: 630216

Supervised by:
Dr. Linnet Taylor
Dr. Colette Cuijpers
Lucas Jones, LL.M

Tilburg, The Netherlands
January 2021
TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND DEFINITIONS .................................................................................. 3

CHAPTER 1 – INTRODUCTION ........................................................................................................... 6

1.1 Problem Statement .................................................................................................................. 6

1.2 Background ............................................................................................................................ 10

1.3 Research Questions ................................................................................................................ 11

1.4 Research Methodology ........................................................................................................... 11

1.5 Research Outline .................................................................................................................... 12

1.6 Interim Conclusion ................................................................................................................ 12

CHAPTER 2 – THE CONCEPT OF PERSONAL DATA PROTECTION UNDER THE INDONESIAN LAWS AND REGULATIONS ..................................................................................... 14

2.1 Introduction ............................................................................................................................ 14

2.2 Sectoral Laws and Regulations ............................................................................................. 14

2.3 Institutions for Data Protection ............................................................................................ 17

2.4 Penalties ................................................................................................................................ 18

2.5 Enforcement .......................................................................................................................... 19

2.6 Interim Conclusion ................................................................................................................ 21

CHAPTER 3 – THE CHALLENGES IN THE ENFORCEMENT OF INDONESIAN PRIVACY AND DATA PROTECTION LAWS ........................................................................................................ 23

3.1 Introduction ............................................................................................................................ 23

3.2 Regulatory Challenges .......................................................................................................... 24

3.3 Institutional Challenge and Accountability Process .............................................................. 26

3.4 Social and Cultural Challenges .............................................................................................. 27

3.5 Recommendation and Measures that can be adopted by Indonesian Government ........... 29

3.6 Interim Conclusion ................................................................................................................ 30

CHAPTER 4 – KEY ELEMENTS TO BE TAKEN INTO ACCOUNT BY THE INDONESIAN POLICYMAKERS IN REGARD TO THE NEED OF A UNIFIED PRIVACY AND DATA PROTECTION LAW ........................................................................................................... 32

4.1 Introduction ............................................................................................................................ 32

4.2 The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) ................... 32

4.3 The Personal Data Protection Act 2012 (PDPA) (Regulation No. 26 of 2012) ................. 35

4.4 Lesson that can be learned from the EU and Singapore ...................................................... 37

4.5 Interim Conclusion ................................................................................................................ 42

CHAPTER 5 - CONCLUSION ............................................................................................................. 43

BIBLIOGRAPHY ............................................................................................................................... 45

ANNEX 1 ........................................................................................................................................ 45
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adminduk Law</td>
<td>Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration/Administrasi Kependudukan</td>
</tr>
<tr>
<td>Advocate Law</td>
<td>Law No. 18 of 2003 on Advocate</td>
</tr>
<tr>
<td>AFPI</td>
<td>Fintech Lender Association/Asosiasi Fintech Pendanaan Bersama Indonesia</td>
</tr>
<tr>
<td>ANRI</td>
<td>National Archives of Republic of Indonesia/Arsip Nasional Republik Indonesia</td>
</tr>
<tr>
<td>Anti-Terrorism Law</td>
<td>Law No. 15 of 2003 on Stipulation of Government Regulation in lieu of Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism, became Law</td>
</tr>
<tr>
<td>Archival Law</td>
<td>Law No. 43 of 2009 on Archival</td>
</tr>
<tr>
<td>ASEAN</td>
<td>Association of South East Asian Nations</td>
</tr>
<tr>
<td>Banking Law</td>
<td>Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking</td>
</tr>
<tr>
<td>BI</td>
<td>Bank Indonesia (Central Bank of Indonesia)</td>
</tr>
<tr>
<td>BIN</td>
<td>State Intelligence Agency/Badan Intelijen Negara</td>
</tr>
<tr>
<td>BI Law</td>
<td>Law No. 23 of 1999 on Bank Indonesia</td>
</tr>
<tr>
<td>BKR</td>
<td>Credit Registration Bureau/Bureau Krediet Registration</td>
</tr>
<tr>
<td>BNN</td>
<td>National Anti-Narcotics Agency/Badan Narkotika Nasional</td>
</tr>
<tr>
<td>Company Documents Law</td>
<td>Law No. 8 of 1997 on Company Documents</td>
</tr>
<tr>
<td>Ditjen Aptika</td>
<td>Directorate General of Informatics Applications/Direktorat Jenderal Aplikasi Informatika</td>
</tr>
<tr>
<td>DNC</td>
<td>Do-Not-Call</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>DPO</td>
<td>Data Protection Officer</td>
</tr>
<tr>
<td>EDPB</td>
<td>European Data Protection Board</td>
</tr>
<tr>
<td>EIT Law</td>
<td>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</td>
</tr>
<tr>
<td>ELSAM</td>
<td>Research and Community Advocacy Institution/Lembaga Studi dan Advokasi Masyarakat</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>EUR</td>
<td>European Monetary Unit</td>
</tr>
<tr>
<td>e-KTP</td>
<td>Electronic-Based Identity Card/Kartu Tanda Penduduk Elektronik</td>
</tr>
<tr>
<td>GBP</td>
<td>Great British Pound</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation (Regulation (EU) 2016/679)</td>
</tr>
<tr>
<td>Code</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>GR 71/2019</td>
<td>Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions</td>
</tr>
<tr>
<td>GR 82/2012</td>
<td>Government Regulation No. 82 of 2012 on the Implementation of Electronic System and Transactions</td>
</tr>
<tr>
<td>HAM Law</td>
<td>Law No. 39 of 1999 on Human Rights/Undang-Undang Hak Asasi Manusia</td>
</tr>
<tr>
<td>Health Law</td>
<td>Law No. 36 of 2009 on Health</td>
</tr>
<tr>
<td>Health Workers Law</td>
<td>Law No. 36 of 2014 on Health Workers</td>
</tr>
<tr>
<td>Hospital Law</td>
<td>Law No. 44 of 2009 on Hospital</td>
</tr>
<tr>
<td>IDR</td>
<td>Indonesian Rupiah</td>
</tr>
<tr>
<td>Indonesian Constitution</td>
<td>1945 Constitution of the Republic of Indonesia</td>
</tr>
<tr>
<td>Intelligence Law</td>
<td>Law No. 17 of 2011 on State Intelligence</td>
</tr>
<tr>
<td>JC</td>
<td>Judicial Commission/Komisi Yudisial</td>
</tr>
<tr>
<td>JC Law</td>
<td>Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission</td>
</tr>
<tr>
<td>KK</td>
<td>Family Certificate/Kartu Keluarga</td>
</tr>
<tr>
<td>Komnas HAM</td>
<td>National Commission of Human Rights/Komisi Nasional Hak Asasi Manusia</td>
</tr>
<tr>
<td>KPK</td>
<td>Corruption Eradication Commission/Komisi Pemberantasan Korupsi</td>
</tr>
<tr>
<td>KPK Law</td>
<td>Law No. 30 of 2002 on Corruption Eradication Commission</td>
</tr>
<tr>
<td>KUHAP</td>
<td>Law No. 8 of 1981 on Criminal Procedural Law/Kitab Undang-Undang Hukum Acara Pidana</td>
</tr>
<tr>
<td>KUHP</td>
<td>Law No. 1 of 1946 on Indonesian Criminal Code/Wetboek van Strafrecht/Kitab Undang-Undang Hukum Pidana</td>
</tr>
<tr>
<td>LGPD</td>
<td>Brazil Lei Geral de Proteção de Dados</td>
</tr>
<tr>
<td>Medical Practice Law</td>
<td>Law No. 29 of 2004 on Medical Practice</td>
</tr>
<tr>
<td>Mental Health Law</td>
<td>Law No. 18 of 2014 on Mental Health</td>
</tr>
<tr>
<td>MoCI</td>
<td>Ministry of Communications and Informatics</td>
</tr>
<tr>
<td>MoCI 20/2016</td>
<td>MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems</td>
</tr>
<tr>
<td>Money Laundering Law</td>
<td>Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime</td>
</tr>
<tr>
<td>Narcotics Law</td>
<td>Law No. 35 of 2009 on Narcotics</td>
</tr>
<tr>
<td>NIK</td>
<td>National Identity Number/Nomor Identitas Kependudukan</td>
</tr>
<tr>
<td>OJK</td>
<td>Financial Services Authority/Otoritas Jasa Keuangan</td>
</tr>
<tr>
<td>OJK Law</td>
<td>Law No. 21 of 2011 on OJK</td>
</tr>
<tr>
<td>PDPA</td>
<td>Singapore Personal Data Protection Act 2012 (Regulation No. 26 of 2012)</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>PDPC</td>
<td>Personal Data Protection Commission</td>
</tr>
<tr>
<td>PID Law</td>
<td>Law No. 14 of 2008 on Public Information Disclosure</td>
</tr>
<tr>
<td>PII</td>
<td>Personally Identifiable Information</td>
</tr>
<tr>
<td>POJK Consumer Protection</td>
<td>OJK Regulation No. 1/POJK.07/2013 of 2013 on Consumer Protection in the Financial Services Sector</td>
</tr>
<tr>
<td>POPIA</td>
<td>South Africa Protection of Personal Information Act</td>
</tr>
<tr>
<td>PPATK</td>
<td>Financial Report and Analysis Center/Pusat Pelaporan dan Analisis Transaksi Keuangan</td>
</tr>
<tr>
<td>Sharia Banking Law</td>
<td>Law No. 21 of 2008 on Sharia Banking</td>
</tr>
<tr>
<td>SIAK</td>
<td>Population Administration Information System/Sistem Informasi Administrasi Kependudukan</td>
</tr>
<tr>
<td>SIM</td>
<td>Subscriber Identification Module</td>
</tr>
<tr>
<td>Telecommunication Law</td>
<td>Law No. 36 of 1999 on Telecommunication</td>
</tr>
<tr>
<td>Terrorism Funding Law</td>
<td>Law No. 9 of 2013 on Prevention and Eradication of Terrorism Crime Funding</td>
</tr>
<tr>
<td>Tipikor Law</td>
<td>Law No. 31 of 1999 on Corruption Eradication/Undang-Undang Tindak Pidana Korupsi</td>
</tr>
<tr>
<td>TPPO Law</td>
<td>Law No. 21 of 2007 on Eradication of Human Trafficking/Undang-Undang Pemberantasan Tindak Pidana Perdagangan Orang</td>
</tr>
<tr>
<td>Trade Law</td>
<td>Law No. 7 of 2014 on Trade</td>
</tr>
<tr>
<td>UK</td>
<td>United Kingdom</td>
</tr>
<tr>
<td>UUPK</td>
<td>Law No. 8 of 1999 on Consumer Protection</td>
</tr>
</tbody>
</table>
CHAPTER 1 – INTRODUCTION

1.1 Problem Statement

Indonesia, a developing country, is currently in the process of digitalizing its economy. The number of internet users and mobile connections in Indonesia has increased significantly over the last several years. In 2018, the total recorded number of internet users in Indonesia was 171.17 million (which implies that 64.8% of the total Indonesian population is online). The highest number of internet users is amongst the youth aged 15-19th (91%) and young adults aged 20-24 years old (88.5%); while the lowest penetration is amongst the elderly aged 60-64 (16.2%) and above 65 years old (8.5%).

The increase of the above also coinciding with the rapid development of e-commerce, marketplace, and digital portal applications in Indonesia. A large amount of foreign and domestic investment has poured into existing tech startups as well as new startups with new business models to monetize and make a profit from this rapidly developing sector.

With regard to the process of digitalizing its economy and monetizing this rapidly developing sector, the Indonesian government and private companies are increasingly engaging in activities that involve the collection and processing of the Indonesian citizens’ personal data. The most visible data collection and processing that have been carried out by them can be illustrated from the following practices: 

1. the collection of development data such as poverty data, population, economic census, and disaster data; 
2. population identity data, namely the electronic-based identity card/kartu tanda penduduk (e-KTP); 
3. subscriber identification module (SIM) card registration for cellphone users; 
4. communication surveillance and direct access to databases; 
5. smart city projects; 
6. election data collected through the voter registration process; 
7. data from medical records and health insurance companies; 
8. financial and taxation data, whether it is collected by banking companies, financial services companies, insurance companies, or tax offices; 
9. transportation data such as the data that is collected by online transportation platform providers; 
10. app usage and social networking; and 
11. e-commerce transactions.

However, at that time, as the collection and processing of the Indonesian citizens’ personal data were conducted under an unclear and uncomprehensive data protection regime, many privacy and data security problems arose.

Some of the problems, without being exhaustive, are as follows:  

1. in early 2018, there was a personal data breach during the registration of mobile SIM cards. The registration process required all SIM cards to be registered using the user’s Citizenship Registration Number/Nomor Induk Kependudukan or Family Certificate/Kartu Keluarga (KK). More than 300 million numbers had already been registered when the data breach was discovered;  
2. in September 2019, approximately 156,000 Indonesian citizens were victims of a breach of passenger data at Malindo Air, a member of the Lion Air group;  
3. during 2018 and 2019, there were 1230 online lending platform providers in Indonesia whose licenses were revoked by the Financial Services Authority/Otoritas Jasa Keuangan (OJK), assisted by the Investment Alert Task Force/Satgas Waspada Investasi due to the misuse of their platforms to access and retrieve personal data.
information not covered under the data collection agreement without the consent of the data subjects involved, for the purposes of debt collection;⁶ (4) there were the sales of personal data gathered from financial institutions, car and property agents/vendors and social media without the consent of data subjects;⁷ and (5) in March 2020, there was a breach involving the medical records of the first Indonesians confirmed to have contracted COVID-19 virus.

Realizing that many problems arising, the Indonesian government has attempted to keep regulatory pace with the development of the data protection regime. Its first step was the enactment of 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). The Indonesian government then enacted several implementing regulations for the EIT Law, including 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). In light of the above, even though the EIT Law and GR 71/2019 contain provisions discussing personal data protection, but these provisions are relatively brief and vague in nature. The closest Indonesia has come is Minister of Communications and Informatics (MoCI) Regulation No. 20 of 2016 on Personal Data Protection in Electronic Systems (MoCI 20/2016). While MoCI 20/2016 provides a more detailed breakdown of the rights and obligations involving personal data protection, it lacks the regulatory power that the law has, such as imposing criminal sanctions.

Like any other country in the world, Indonesia is currently moving slowly to provide a comprehensive data protection regime, where a new data protection law is going to be issued immediately to tackle the problems that have arisen and to prevent and minimize the possibility of any data security issues in the future. The planning of the new law issuance raises the questions of how the current Indonesian data protection regime is, what challenges are faced by the Indonesian government in implementing the current data protection regime, how are the data protection regime that protects personal data in other countries, and what key provisions that are important and should be incorporated to the said new law to boost a greater level of enforcement.

It is pertinent to note that in the current Indonesian legal system, there is no single unified regulation concerning personal data protection⁸ as the data protection legislations are scattered across various governmental and sectoral regulations, and are not unified under one comprehensive regulation, such as the European Union’s (EU) General Data Protection Regulation (GDPR). The work of the Research and Community Advocacy Institution/Lembaga Studi dan Advokasi Masyarakat (ELSAM) highlights the disharmonized state of Indonesian data protection law, with at least 30 regulations containing the personal data protection provisions which tend to overlap each other.⁹

The overlapping of the abovementioned regulations can be seen from the following aspects: (a) purpose of personal data processing; (b) notification or consent of the data subject; (c) retention period of personal data; (d) erasure or alteration of personal data; (e) the disclosure of personal data to third parties; (f) sanctions for violators of the relevant regulations; (g) recovery mechanisms for victims of privacy rights violations.¹⁰ These aspects overlap in the sense that several regulations regulate the same concepts as regulated by the other regulations. For example, both the EIT Law and the Banking Law have the provisions of the notification or consent of the data subject, the disclosure

---

⁶ Otoritas Jasa Keuangan (Financial Services Authority), ‘Otoritas Jasa Keuangan Dan BARESKRIM POLRI Sepakat Berantas Fintech Peer-To-Peer-Lending Ilegal Dan Investasi Ilegal’ (Satgas Waspada Investasi 2019).
⁷ K&K Advocates, ‘Unauthorized Transfer Of Personal Data Might Be Punishable Under The Indonesian Criminal Law’.
⁹ These regulations are scattered across various sectors, such as telecommunications, banking, finance, taxation, population, filing, law enforcement, security, and healthcare.
¹⁰ Djafar (n 2).
of personal data to third parties, and sanctions for violators of the relevant regulations. However, since each law has limited scope for each sector (not general), the aspects that have been regulated in the EIT Law are similar to the concepts regulated by the Banking Law, where it does not complete each other in providing comprehensive protection. Therefore, though there are two or more regulations that regulate the same aspects, both regulations still fail to come together to provide comprehensive personal data protection.\footnote{Wahyudi Djafar, Bernhard 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.} Due to these overlapping conditions, there is no uniform national definition of personal data in Indonesia, as each sectoral regulation contains its own definition. For example, in Population Administration Law and the Government Regulation on System and Electronic Transaction Organizer, personal data is defined as specific individual data in which authenticity and confidentiality are stored and protected. However, under other regulations, such as Banking Law, Sharia Banking Law, and Telecommunication Law, the definition of personal data is only related to the information of debtors, investors, as well as the records of telecommunications services.

Digging deeper into the possible challenges faced by the Indonesian government, the complexity of the current overlapping regulations can already be considered as a regulatory challenge for the Indonesian government in implementing and enforcing the current data protection regime. The existence of this regulatory challenge somehow raises the questions of whether that is the only challenge or there are any other challenges that are currently being faced by the Indonesian government, as well as what are the possible measures that can be adopted by the Indonesian government to overcome the current challenges and to prevent the possible upcoming challenges. Apart from the regulatory challenges, the possible issues that might arise are the overlapping responsibilities of the sectoral regulator as well as their capabilities of regulating the privacy and data protection concept, especially when the regulator-in-charge is also the Indonesian citizens that might not be yet deeply aware regarding such particular concept. Therefore, it is necessary to gain a deeper understanding regarding the abovementioned issues or challenges that later will be referred to as an institutional challenge, and social and cultural challenges.

On a separate note, despite the existing various sectoral regulations in Indonesia, Indonesian scholars, privacy advocates, and research institutions do not regard these regulations as adequate or sufficient because the regulation is considered as too broad and unclear, as well as limited in scope as elaborated earlier.\footnote{Ibid.} Further, referring back to the case studies above, an adequate degree of the applicable data protection regulations was reflected, but it is not sufficient to protect the personal data of the Indonesian citizens because those various sectoral regulations were not specifically designed to cover the data protection-related-matters. The provisions stipulated in such regulations are just merely on a surface level without having a thorough elaboration on how it should be implemented (in a technical manner).

The inadequacy of the current data protection regime was also acknowledged by some of the government officials. Noor Iza, the head of the Sub-directorate of e-Business Technology and Infrastructure at the MoCI, stated that the protection of personal data had not been regulated by the law but only in government regulations, and it is necessary to ensure the harmonization of data protection law.\footnote{Supriyadi Widodo Eddyono and Wahyudi Djafar, ‘Menyeimbangkan Hak: Tantangan Perlindungan Privasi Dan Menjamin Akses Keterbukaan Informasi Dan Data Di Indonesia’.} Additionally, Evita Nursanty, the Commission 1 Member of the Indonesian House of Representatives, also stated that it is essential to have a data protection law as the current regulations are not sufficient in protecting our data.\footnote{PDSI KOMINFO, ‘Komisi I: Indonesia Perlu UU Perlindungan Data Pribadi’ [Official Website of Ministry of Communication and Informatics, 2017] <https://kominfo.go.id/content/detail/11715/komisi-i-indonesia-perlu-uu-perlindungan-data-pribadi/0/sorotan_media> accessed 26 December 2019.} Fortunately, the abovementioned concerns, together with the increasing demands from various government and non-governmental institutions, have been
brought to the Indonesian government’s attention, and they are currently in the process of drafting a data protection law.\textsuperscript{15} Indonesia will have its own data protection law soon and will become the fifth country in the Association of South East Asian Nations (ASEAN) to implement such data protection law.\textsuperscript{16}

Based on my research, a comprehensive and competent data protection regulation, should at the very least, contain the following aspects: (1) the principles of lawfulness, fairness, and transparency of processing; (2) the purpose limitation principle; (3) the data minimization principle; (4) the data accuracy principle; (5) the storage limitation principle; (6) the data security principle; (7) accountability principle; (8) the independent supervision; (9) data subject rights and their enforcement; (10) obligations of controllers and processors; and (11) international data transfers and flows of personal data.\textsuperscript{17} On a separate note, there are a lot of countries in the world that this year made their data protection law coming into effect, such as Brazil’s \textit{Lei Geral de Proteção de Dados} (LGPD), Thailand’s PDPA, South Africa’s Protection of Personal Information Act (POPIA), as well as some countries that are going through the final approval stages in 2020 like India, it is important and necessary for Indonesia, as the country that is just starting its journey to provide better data protection framework for their citizens, to learn from the other countries or unions that have understood and implemented the concept of data protection in the form of one comprehensive regulation, such as the EU with their GDPR and Singapore (for example from ASEAN country perspective) with their PDPA, as they provide a detailed regulatory regime concerning personal data and have influenced personal data regulations worldwide.\textsuperscript{18}

The GDPR can be a perfect example of competent and comprehensive data protection regulation as it has all the abovementioned aspects and the fact that its enforcement is well implemented. In this regard, having the GDPR as the example to be discussed and examined will add more insight and knowledge that can be learned by the Indonesian policymakers. Besides that, as mentioned above, Singapore’s PDPA can also be taken as an example to provide further knowledge on how the data protection regulations being regulated and enforced in the ASEAN territory. Discussing Singapore’s PDPA, content-wise, it shares many of the GDPR’s key provisions that are introduced under different terms and added by a special provision that is rarely be found in other countries’ data protection laws or regulations. In Singapore’s PDPA, the abovementioned aspects are called as “obligations” (instead of principles, as referred to in the EU’s GDPR) that is regulated under different and separate articles, as follows: (1) the consent obligation; (2) the purpose limitation obligation; (3) the notification obligation; (4) the access and correction obligations; (5) the accuracy obligations; (6) the protection obligation; (7) the retention limitation obligation; (8) the transfer limitation obligation; and (9) the accountability obligation. Besides these obligations, Singapore’s PDPA also provides a special provision called as Do-Not-Call (DNC) registry provision, a provision which generally prohibits any organizations from sending certain marketing messages (in the form of voice calls, text, or fax messages) to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers, registered with the DNC registry.\textsuperscript{19} Another important consideration to learn from the abovementioned regulations is that the business sector also prefers to refer to the GDPR and PDPA as the main sources for developing their data protection policies.\textsuperscript{20}

\textsuperscript{15} Supriyadi Widodo Eddyono and Wahyudi Djafar, ‘Menyeimbangkan Hak: Tantangan Perlindungan Privasi Dan Menjamin Akses Keterbukaan Informasi Dan Data Di Indonesia’.


\textsuperscript{18} ibid.

\textsuperscript{19} Personal Data Protection Commission - Singapore, ‘ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT’.

\textsuperscript{20} Putri (n 1).
Therefore, the application of the abovementioned aspects by the data protection regimes of the EU and Singapore, which can potentially resolve existing problems in Indonesia such as the disclosure of data without consent and another existing problem in current Indonesia's data protection regime, is what I believe Indonesian law must ensure while drafting and implementing its upcoming data protection law. However, the Indonesian policymakers should take into consideration the shortcomings of the abovementioned data protection regulations as well while bringing in a new data protection regime. For instance, it is pertinent to note that the PDPA does not cover governmental uses of data, and hence it would be feasible if the Indonesian policymakers deviate from the PDPA's lack of inclusion with respect to the governmental uses of data. Hence, the most appropriate way for Indonesia is to create uniform legislation that covers all aspects of data protection, as mentioned in the GDPR and the PDPA, while considering the pitfalls at the same time.

1.2 Background

The concept of privacy is admittedly elusive, which most individuals would agree in the context of human rights, the personal data must be protected by the responsible party such as individuals, government, and the business organizations. But it is difficult to achieve a situation where everyone agrees upon the limitation and restriction of privacy. Presently, the concept of privacy within the boundaries of the legal system still in its development stage due to technological advancement. The concepts of privacy and data protection have been acknowledged for a long time in Indonesia. The fundamental basis for these concepts can be found in Article 28(G) of the 1945 Constitution of the Republic of Indonesia (Indonesian Constitution), which states that every person has the right to (1) protection of themselves, their families, respect, dignity and possessions under their control; and (2) security and protection from the threat of fear for doing, or not doing, something that constitutes a human right. Even though the Indonesian Constitution does not explicitly mention the concept of privacy and data protection, this article can be considered as a legal basis for more specific data protection laws and regulations.

In 2008, Indonesia enacted its first cyberlaw, the EIT Law, to provide legal certainty and foothold to enhance the electronic transaction security on the internet and within Indonesia’s boundaries. As time goes by, the Indonesian government issued quite a number of sectoral regulations, each of which stated provision(s) that indirectly contained privacy and data protection principles and concepts. However, such numbers of regulations are considered deficient and have not succeeded in protecting Indonesian citizens’ personal data as it is not specific and unclear. In comparison to the other countries, most of them already have specific laws to protect the privacy and personal data of their citizens. For instance, the GDPR in the EU and PDPA in Singapore which provide a detailed regulatory regime concerning personal data and have influenced personal data regulations worldwide for the provisions that they designed and implemented. A comprehensive and unified regulation concerning privacy and data protection could be considered as one of the most important areas of need in Indonesia as it is one of the major issues in the modern community that needs to be addressed urgently and immediately. Even though the Indonesian government is currently preparing the new unified data protection law, it is necessary to ‘look at the mirror’ and understand further regarding how the personal data protection concept is currently being regulated and implemented, the challenges faced in enforcing the current personal data protection regime, and what can be

---

24 Hoofnagle, Sloot and Borgesius (n 17).
learned from the EU’s GDPR and Singapore’s PDPA to improve the data protection frameworks in Indonesia.

Therefore, the principle objective of this thesis is to provide insights on what needs to be incorporated in a new unified data protection regulation in Indonesia with respect to data protection based on the key concepts of the EU’s GDPR and Singapore’s PDPA to resolve the inconsistencies arising out the existing patchwork of laws regarding Indonesian data protection regime.

1.3 Research Questions

From the Problem Statement and Background given above, the following is the main research question: “What are the significant drawbacks in the current Indonesian data protection framework and what elements of the regimes of the EU and Singapore and be relied upon to rectify these drawbacks?”

To better understand and answer this research question, I consider the following sub-questions:

1) How is the personal data protection concept currently being regulated under the Indonesian laws and regulations, and how are the relevant Indonesian laws and regulations implemented?

2) What are the challenges faced in enforcing the current personal data protection regime in Indonesia, and what measures can be adopted by the Indonesian government to address these concerns effectively?

3) What lessons can Indonesian policymakers learn from the European Union’s GDPR and Singapore’s PDPA?

1.4 Research Methodology

In order to answer the main research question and the sub-questions above, the methodologies that will be used in this thesis are doctrinal research, comparative research and empirical research.

The doctrinal legal research was chosen as the primary method because any legitimate answer to the main research question and the sub-questions can only result from the systematic analysis of legislation, case law, and literature. By using the doctrinal legal research, I will assess the data protection legislation in Indonesia from both ends of the hierarchy, from the upper (the 1945 Indonesian Constitutions and its amendments) as well as the lower hierarchy (the Government Regulation and Ministerial Regulation). The assessment of the data protection legislation in this regard is not only limited to the Indonesian legislation but also covers the legislation from the EU and Singapore for the purpose of comparison. Furthermore, as the doctrinal research will help me to thoroughly analyze the relevant legal texts to interpret what law exists regarding the particular context, thus, it is well suited to be used for sub-questions 1 and 3.25 For sub-question 1, it is necessary to understand the relevant Indonesian regulations as mentioned earlier before moving forward to answer the specific questions of “how is the personal data protection concept being regulated under the Indonesian laws and regulation, and how are the relevant Indonesian laws and regulations implemented?”. As for sub-question 3, it is also necessary to understand the basic features of EU’s GDPR and Singapore’s PDPA before the question of “what lessons can Indonesian policymakers learn from the EU and Singapore experiences on personal data protection?” can be answered.

With regard to the above, comparative research will also be conducted in this thesis. The privacy and data protection legislation in Indonesia will be compared and analyzed with equivalent regulations in the EU and Singapore, in order to provide the reader with a deeper understanding of how the legal framework in these regimes protects the personal data of the citizens. Furthermore, it will highlight the similarities and differences in legislative approaches towards the existing data protection regime in these nations. The comparative research will help me identify the lessons that Indonesian policymakers can learn from the EU and Singapore’s experiences on enforcing their privacy and data protection regimes. This specific research method will be used to answer sub-question 3.

I will also use empirical research as part of this thesis, for evidence regarding the subject matter based on observation and experience. The empirical research is necessary to answer sub-question 2, where the empirical evidence from the existing court cases and news reports in both printed and online media are needed to conduct a further assessment of the risks and challenges faced by the Indonesian government in enforcing Indonesian data protection regime and to seek further possible measures that can be adopted by the Indonesian government to effectively address such risks and challenges.

1.5 Research Outline

For the purpose of answering the research questions laid above, this research will be structured in the following manner:

Chapter 2 of the thesis will provide an explanation of how the concept of personal data protection is being regulated under the Indonesian laws and regulations and how the relevant Indonesian laws and regulations are implemented. I will list and explain in detail the various regulations which concern privacy and data protection, which will further be followed by case studies related to the exploitation and abuse of Indonesian citizens’ personal data.

Chapter 3 of the thesis will contain a discussion of the challenges faced in enforcing the current personal data protection regime in Indonesia. In this regard, I will list and explain in detail the risks and challenges that are currently faced by the government institutions in enforcing the current data protection regulations in Indonesia. An analysis of the case studies that have been elaborated in Chapter 2 will also be provided, based on which I will list and explain several possible measures that can be implemented by the Indonesian government to address the risks and challenges in enforcing such data protection regulations in Indonesia.

Chapter 4 of the thesis will contain the assessment of the legal framework that protects personal data in the EU and Singapore. From this assessment, I will provide an analysis of what lessons can be learned by Indonesian policymakers from these regimes.

Chapter 5 of the thesis will conclude all the previous sub-questions to answer the main question. This will answer how effective are the existing Indonesian data protection laws and regulations protection compared to the data protection regime of the EU and Singapore.

1.6 Interim Conclusion

This chapter has reflected the background and problem statement of this thesis, where it elaborated the preliminary concept of privacy and data protection that has been acknowledged in Indonesia where the privacy and data protection issues have emerged and become an increasing concern due to the way the government and private companies collect and process personal data without the adequate and comprehensive data protection regime, which leads to the misuse of the

collected personal data. This thesis will provide an analysis on how is the latest implementation of the existing data protection regime in Indonesia, its weaknesses, risks, and challenges faced in enforcing the existing data protection regime, as well as the lessons that can be adopted by Indonesian policymakers from the EU and Singapore’s experience, in order to understand what is best for Indonesia and how Indonesian data protection regime should be architected in the future. Furthermore, in the next chapter, I will elaborate in detail regarding how the data protection concept being regulated under the Indonesian laws and regulations and how such laws and regulations implemented.
CHAPTER 2 – THE CONCEPT OF PERSONAL DATA PROTECTION UNDER THE INDONESIAN LAWS AND REGULATIONS

2.1 Introduction

The protection of personal data in Indonesia was initially considered as an extension of the right to privacy. Under the Indonesian Constitution, the concept of the right to privacy has been recognized and protected under the general concept of human rights. Further, with the need to regulate internet and electronic transaction-related activities, The EIT Law was passed. Even though most of the EIT Law provisions focus on electronic transactions, it does contain a specific provision on personal data protection.27

Article 26(1) of the EIT Law (along with its official elucidation) recognizes personal data protection as a part of privacy rights. Further, it states that privacy rights shall include, among others, the right to monitor the access of information concerning private life and data. To further satisfy the need for the adequate protection of personal data, the MoCI issued MoCI 20/2016. MoCI 20/2016 is issued as mandated by Article 15(3) of GR 82/2012 as amended by the GR 71/2019, which requires personal data protection in electronic systems to be regulated by a ministerial-level regulation. MoCI 20/2016 came into effect on 1 December 2018 and applied only to Personally Identifiable Information (PII) stored in electronic systems but not to PII that is stored manually.28

Besides the above legislation, privacy and personal data protection are also included in several laws and regulations, though most of these laws and regulations only cover these concepts briefly. The contents of these laws and regulations can be seen in Annex 1 of this thesis.

At least 30 statutory regulations explicitly and implicitly recognize the concept of privacy and data protection. Several regulations confirm that the right to privacy and the right to data protection can be restricted for law enforcement purposes and by certain job positions or designations. For example, in the KUHAP, the police have the authority to access someone’s private letter if such letter is suspected related to an ongoing criminal investigation, and also in the Healthcare Law, where one’s right to privacy towards the medical records can be disclosed to the public for the sake of law enforcement interests.

2.2 Sectoral Laws and Regulations

In the Indonesian legal system, there is no single unified regulation concerning personal data protection as the data protection legislation is scattered across various sectoral regulations and not unified under one comprehensive regulation such as the EU’s GDPR.29

Apart from the 30 regulations that recognize privacy and data protection as mentioned above, the EIT Law, MoCI 20/2016, and GR 71/2019 are only applicable to all data processing or usage of personal data in electronic form by Electronic System Providers (ESPs), which is defined as any person, state administrator, business entity, or community that provides, manages or operates an electronic system, whether individually or jointly, for the electronic system’s users’ own interests or the interests of other parties. For this definition, electronic systems are defined as a series of devices and electronic procedures used to prepare, collect, process, analyze, store, display, announce, deliver, or disseminate electronic information.30

Although processing or usage of personal data in a manual record is excluded from the scope of the above regulations, ESPs are responsible for complying with the relevant regulations, regardless

27 Aaron P Simpson and others, ‘Data Protection & Privacy - 2020’.
28 ibid.
29 Rosadi (n 23).
30 Simpson and others (n 27).
of the sectors or type of organizations, with respect to the protection of personal data stored in their electronic system.

As a fundamental principle, Indonesia adopts a consent-based regime to obtain and process personal data through electronic systems. Prior consent of the data subject is unnecessary if the personal data collection is mandated by law or if certain personal data has been transmitted publicly by electronic systems for public services.

Certain exemptions are also applicable in the Banking and Finance sector, where banks are required to maintain the confidentiality of information concerning the savings and deposits of customers, except for exceptional circumstances; namely, taxation purposes, settlement, claims, and interbank exchanges of information.\textsuperscript{31} The above-mentioned regulations will be divided into eight sub-sections and elaborated below.

**Human Rights:** This includes the KUHP, HAM Law, and TPPO Law. Each regulation provides some personal data protection to the relevant party. They are either addressed towards citizens or might specially regulate the officials’ obligation to protect personal data and its limitations. For example, KUHP regulates civil servants’ or officials’ obligation to uphold the value of someone’s personal data when performing their duties.\textsuperscript{32} On the other hand, the HAM Law emphasizes a more general idea of human rights derived from the Indonesian Constitution by recognizing the personal protection of citizens in the context of family, honor, dignity, property rights, and the right of “should not be disturbed” or “right to privacy”.\textsuperscript{33} The TPPO provides a different approach to data protection. It focuses more on limiting the intrusion on data protection in the context of wiretapping and the access of personal data of human trafficking suspects,\textsuperscript{34} which implies that there are measures from the state to prevent the misuse of one’s personal data, despite the absence of a unified data protection regulation.

**Telecommunication and Media:** This includes the Telecommunication Law, EIT Law, and PID Law. Telecommunication Law regulates the legal protection of the citizens’ right to privacy and data protection in the context of communications. The telecommunication service providers must maintain the confidentiality of information of their users. However, wiretapping is allowed on the submission of a written request from an authorized legal enforcer such as an attorney or the police.\textsuperscript{35} Further, the EIT Law regulates internet and electronic transaction activities but also recognizes the right to privacy to some extent. The EIT Law states that privacy rights shall include, among others, the right to monitor the access of data concerning the private life of a citizen.\textsuperscript{36}

Whereas the PID Law’s approach towards data protection is focused more on regulating the obligation to protect the information relating to personal rights by giving authorities the power to control the activities of public agencies pertaining to the public disclosure of personal data while maintaining, upholding, and protecting the value of such personal data.\textsuperscript{37}

**Security and Defense:** This includes the Anti-Terrorism Law, Intelligence Law, and Terrorism Funding Law. The Anti-Terrorism Law allows investigators to access details concerning the assets of

\textsuperscript{31} More elaboration can be found in the Banking and Finance sub-section or Annex 1 of this thesis.
\textsuperscript{32} Article 430-333 of Law No. 1 of 1946 on Indonesian Criminal Code.
\textsuperscript{33} Article 31-32 of Law No. 39 of 1999 on Human Rights.
\textsuperscript{34} Article 31-32 of Law No. 21 of 2007 on Eradication of Human Trafficking.
\textsuperscript{35} Article 40-42 of Law No. 36 of 1999 on Telecommunication.
\textsuperscript{36} Article 26(1) of Law No. 11 of 2008 on Electronic Information and Transactions.
\textsuperscript{37} Article 6(3)(c) of Law No. 14 of 2008 on Public Information Disclosure.
parties suspected of, or known for committing acts of terrorism.\textsuperscript{38} This law regulates the intrusion procedures albeit without a clear limitation on the extent of data that can be accessed by the authorities, which can lead to the misuse of this provision.

A similar situation is observed in the Intelligence Law. The BIN is given the authority to conduct wiretapping and investigate the flow of funds and information from suspicious activities occurring in Indonesia, whereby the BIN can request law enforcers and related institutions for such information.\textsuperscript{39} This provision contains some potential for misuse as it fails to provide a clear limitation on the data that authorities can access. The Terrorism Funding Law provides some authority to law enforcers to observe and access the citizens’ personal data, who are suspected of committing terrorism, which can also be misused to violate citizens’ right to privacy.

\textbf{Justice}: This includes the KUHAP, Tipikor Law, KPK Law, Advocate Law, and JC Law. While the KUHAP allows the violation of the right to privacy in certain cases, it also provides a degree of data for the data subject as reflected from the safeguards that provide access to personal data only through special judicial permission and limit such access only to certain data. The Tipikor Law does not discuss a detailed privacy and data protection mechanism for the suspect and his family. However, this law emphasizes that the identities of a witness and the parties of proceedings must not be disclosed, thereby protecting their personal data. The KPK Law regulates that the KPK has the authority to wiretap and record the communication contents of the suspects or defendants. However, this law indirectly limits investigators’ access to the personal data of the suspects and defendants, as the data can only be accessed if such it is related to the acts of corruption acts such as tax and asset records. Advocate law regulates the private relationship between advocates and clients, discussing the advocates’ obligation to protect their clients’ confidentiality unless otherwise specified by law.\textsuperscript{40} JC Law allows for the wiretapping or recording of the judge’s conversation if there is an alleged violation of the judicial code of ethics.\textsuperscript{41}

\textbf{Archives and Population}: This includes the Adminduk Law and Archival Law. Adminduk Law regulates the obligation of the state to maintain and protect the personal data of the population through the census, civil registration, and other activities that related to the collection and storage of population-related personal data,\textsuperscript{42} but has not fully accommodated the protection of the personal data of the population. The Archival Law regulates the archiving of public documents in the state administrative organizations to ensure the safety and security of personal data in the state archives.\textsuperscript{43}

\textbf{Health}: This includes the Medical Practice Law, Narcotics Law, Health Law, Hospital Law, Mental Health Law, and Health Workers Law. All of these laws require the doctor to maintain the confidentiality of the patient’s health data and medical records unless such documents must be disclosed for the sake of law enforcement.\textsuperscript{44} \textsuperscript{45} \textsuperscript{46} However, the Narcotics Law adopts a different approach by regulating the procedures and requirements of interfering with the citizens’ right to

\textsuperscript{38} Article 30 of Government Regulation in lieu of Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism.
\textsuperscript{39} Article 31 of Law No. 17 of 2011 on State Intelligence.
\textsuperscript{40} Article 19 of Law No. 18 of 2003 on Advocate.
\textsuperscript{41} Article 20(3) of Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission.
\textsuperscript{42} Article 85 of Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration.
\textsuperscript{43} Article 3(f) of Law No. 43 of 2009 on Archival.
\textsuperscript{44} Article 47(2) of Law No. 29 of 2004 on Medical Practice.
\textsuperscript{45} Article 57 of Law No. 36 of 2009 on Health.
\textsuperscript{46} Article 58(1) of Law No. 36 of 2014 on Health Workers.
privacy such as carrying out the wiretapping and accessing the wealth and taxation data related to suspects of misuse of and illicit trafficking of narcotics and narcotics precursors. 47

**Banking and Finance:** This includes the Banking Law, BI Law, Sharia Banking Law, Money Laundering Law, and OJK Law. The Banking Law interprets bank secrets as everything related to the information regarding customers and their deposits. 48 Sharia Banking Law also regulates similar matters but through the sharia approach. Both laws oblige the banks to maintain the principle of confidentiality of their customers and their deposits. The BI Law briefly regulates both conventional and sharia banks’ activities in Indonesia. It includes regulating the obligation of banks to maintain the confidentiality of its customers’ personal data. 49 The Money Laundering Act allows the PPATK to intrude on citizens’ right to privacy to prevent and eradicate money laundering. 50 The interesting fact here is that the laws regulating the bank’s secrecy and other financial transactions do not apply to the investigators, prosecutors, and judge in charge. Therefore, I believe that there is a contradiction between the personal data regulations discussed in the Banking Law, Sharia Banking Law, BI Law, and the Money Laundering Law.

**Trade and Industry:** This includes the Company Documents Law, Consumer Protection Law, and Trade Law. While the Company Documents Law does not specifically regulate the protection of personal data, it does provide some protection in the form of providing a document retention period and the deletion mechanism of such documents. Furthermore, the current trading practices reflect that consumers’ personal data is frequently obtained when they use a service or purchase an item or goods. For example, when conducting online transactions, the consumer must provide their personal information to complete the transaction process. Later on, the submitted personal information can be misused. However, I believe that the Consumer Protection Law was not designed comprehensively to prevent the abuse of personal data as it was issued in 1999, where the purpose of such law was to raise awareness on consumer rights in general. This law prohibits false offerings, production, and advertisements of goods and/or services. No provision provides a remedy for consumers whose personal data has been abused. As for Trade Law, it does not regulate the protection of consumers’ personal data but states that for trading activities involving an electronic system or e-commerce, traders must refer to any applicable provision as stipulated in the EIT Law. 52 It means that the EIT Law provisions regarding the protection of customers’ personal data are also fully binding for trades that take place on electronic systems.

### 2.3 Institutions for Data Protection

Until now, there has been no specifically dedicated national data protection authority that oversees the protection of personal data in Indonesia. However, pursuant to MoCI 20/2016 (along with the Directorate General of Informatics Applications or Ditjen Aptika) is responsible for ensuring compliance with Indonesia’s data protection regime (i.e., EIT Law, GR 71/2019, and MoCI 20/2016). 53

The MoCI is authorized to organize governmental events related to communications and informatics; coordinate with ESPs for transfer of personal data overseas; settle disputes related to

---

47 Article 75(i) of Law No. 35 of 2009 on Narcotics.
48 Article 1(28) of Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking.
49 Article 24 of Law No. 23 of 1999 on Bank Indonesia.
50 Article 27 of Law No. 23 of 1999 on Bank Indonesia.
51 Article 72 of Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.
52 Article 65(3) of Law No. 7 of 2014 on Trade.
53 Simpson and others (n 27).
failure or breach of PII protection; supervise the implementation of personal data protection; request data and information from ESPs in the framework of data protection; impose administrative sanctions for violations of data protection laws and regulations; and issue Electronic System Worthiness Certificate to certify that an electronic system is functioning properly.\textsuperscript{54}

For certain specific matters, such as disputes related to a breach of personal data, the MoCI may delegate its authority to Ditjen Aptika, which is authorized to form a panel to settle the dispute and recommend certain administrative sanctions to be imposed by the MoCI on relevant ESPs. Ditjen Aptika is also responsible for raising public awareness on matters related to personal data protection.\textsuperscript{55} Since the main data protection regulations were enacted, public awareness has been increased and maintained by holding seminars related to data protection issues.

In addition, for a specific sector (e.g., financial sector), each sectoral supervision and regulatory body has the internal authority to regulate the relevant matters related to data protection. The authority to oversee and supervise data processing can also be seen in several regulations. These provisions do not explicitly discuss the obligation to protect data but only focus on the oversight of processing activities without elaborating on the standards to be maintained while facilitating such oversight. However, several regulations discuss the details of the protection mechanism in various ways. For example, in KUHAP and EIT Law, the authority of the police must be based on the decision of the Chairman of the District Court. However, in the Money Laundering law and KPK Law, the authority of PPATK and KPK in accessing one’s personal data can still be carried out even without a prior order or permission of the Chairman of the District Court, as long as their investigators have obtained sufficient preliminary evidence. As for the Banking and Finance Sector, all banking activities, conventional or sharia, are supervised by the BI, while the supervisory authority has been transferred to the OJK. In this regard, the supervision includes bank’s obligation to maintain the confidentiality of their customers’ personal data.

With regard to the cooperation with other data protection authorities, under MoCI 20/2016, the MoCI may coordinate with the sectoral supervision and regulatory body to follow up on complaints lodged by data subjects involving failures of personal data protection committed by ESPs. These two authorities may also cooperate in supervising the implementation of MoCI 20/2016, including the imposition of administrative sanctions for breaches of MoCI 20/2016. Under MoCI 20/2016, the MoCI delegates the authority to settle PII disputes to Ditjen Aptika, which may then form a panel to do so. The MoCI also delegates the supervision of the implementation of the MoCI 20/2016 to Ditjen Aptika.\textsuperscript{56}

Particularly for cooperation with foreign authorities in certain specific matters, such as transnational data transfer, there is no evidence of the existence of any cooperation entered into by the MoCI with foreign authorities at present, nor has the Indonesian government published a list of countries considered to have an adequate level of protection concerning transnational data transfer.

\textbf{2.4 Penalties}

The breaches of data protection laws, as mentioned above, may vary. After a further assessment of such laws, the breaches of data protection law will lead to administrative sanctions or orders and criminal penalties. It will depend on the provisions of each law as such law is limited to its sectoral capability. Therefore, any data protection-related matters stipulated under those laws will mostly only cover specific sectoral value and will not generally apply, though some are related to each other.

\textsuperscript{54} ibid.
\textsuperscript{55} ibid.
\textsuperscript{56} ibid.
Breach of data protection might be subject to administrative and criminal liability in Indonesia. As a rule of thumb, under MoCI 20/2016, any person that collects, processes, analyses, stores, promotes, announces, transmits, or publishes personal data without the right to do so will be subjected to certain administrative sanctions, such as verbal warning; written warning; suspension of activities; or announcement on the MoCI’s website stating that the party has not complied with data protection regulations. Failure to comply with GR 71/2019 will also be subjected to similar administrative sanctions, comprising a written warning, administrative fines; temporary dismissal; or dismissal from the list of registrations.

Under the EIT Law, a breach of data protection is also subject to criminal penalties, such as a fine of Indonesian Rupiah (IDR)600,000,000 (six hundred million Indonesian Rupiah) up to IDR800,000,000 (eight hundred million Indonesian Rupiah) and 6 to 8 years’ imprisonment for unlawful access, a fine of IDR2,000,000,000 (two billion Indonesian Rupiah) up to IDR5,000,000,000 (five billion Indonesian Rupiah) and 8 to 10 years’ imprisonment for alteration, addition, reduction; transmission, tampering, deletion, moving or hiding electronic information or electronic records, a fine of IDR800,000,000 (eight hundred million Indonesian Rupiah) and 10 years’ imprisonment for interception or wiretapping of a transmission, and a fine of IDR10,000,000,000 (ten billion Indonesian Rupiah) to IDR12,000,000,000 (twelve billion Indonesian Rupiah) and/or 10 to 12 years’ imprisonment for the manipulation, creation, alteration, destruction or damage of electronic information and/or electronic documents with the purpose of creating an assumption that such electronic information and/or documents are authentic (for instance, anyone will be imprisoned if he alters a counterfeit electronic document to make the information contained within it look authentic), and other violations related to the processing of electronic information and/or documents.

In addition, under the Telecommunication Law, any person is prohibited from wiretapping information transmitted through telecommunication networks. A person violating this prohibition may be sentenced to imprisonment of up to 15 years. Note that other sectoral laws have more specific sectoral data breach sanctions.

In the event of a data breach, several regulations regulate different types of sanctions, from criminal sanctions to administrative sanctions. For example, Telecommunication Law and Terrorism Funding Law provide criminal sanctions for those who leak or disclose confidential data or information. Further, Intelligence Law and KPK Law provide criminal sanctions and fines for the abuse of wiretapping authority, which constitutes an intrusion of a citizens’ right to privacy.

2.5 Enforcement

In this sub-section, I will provide some brief examples of cases where enforcement has occurred concerning the legal instruments that have been discussed above. However, more detailed issues related to the enforcement such as challenges will be provided later in the following chapter of this thesis.

With respect to the enforcement of the above laws, the MoCI can only commence an investigation after receiving a complaint from a data subject and/or ESPs. The complaint can be filed on the grounds that a data breach exists. The dispute will then be settled by the data privacy dispute settlement panel formed by the Ditjen Aptika, with all the parties involved. As there are no clear standards or criteria for the “loss” threshold caused by the data breach, disputes are settled on a case-

57 Rahmansyah and Nabila (n 22).
58 Simpson and others (n 27).
59 Simpson and others (n 27).
60 Rahmansyah and Nabila (n 22).
61 More elaboration can be found in Annex 1 of this thesis.
by-case basis. The GR 71/2019 and MoCI 20/2016 do not provide any right of appeal to this dispute settlement panel’s decision.

In light of the above, the following are the data protection-related cases that have recently taken place in Indonesia, to provide a further understanding of how data protection-related cases are being settled through various approaches based on the current regulations in Indonesia.

**Buni Yani Case:** The Indonesian Police’s cybercrime unit has become quite aggressive in investigating cybercrimes pertaining to malicious comments, defamation of character, and hoaxes, especially those interfering with national interests. One of the most recent high-profile enforcement cases relating to cybercrime involved Buni Yani, a former lecturer at a private university in Jakarta, who was convicted of violating Article 32 of the EIT Law for editing an electronic document so that the altered document was publicly accessible. The case was opened following a public outcry over Buni editing a video of a gubernatorial candidate’s speech to make it appear that the candidate had committed an act of blasphemy and then uploading the video to the internet. The prosecution in the case presented several electronic documents as evidence, namely a screenshot of Buni’s social media account, his email account, mobile phone, and the video uploaded to the internet. The defendant was sentenced to 18 months in prison.

**Hacking Cases:** In 2013, a 19-year-old man was sentenced to six months in prison and fined after he was found guilty of hacking the official website of a former president of Indonesia. Another hacker was sentenced to 15 months in prison after he was found guilty of hacking the Indonesian Press Council’s official website.

**Unauthorized Data Transfer Case:** A recent judgment by the District Court of Tangerang shows that the unauthorized transfer of personal data is subjected to criminal sanctions. The court issued a verdict against Abi Warnadi Ismentin, who sold personal data without securing personal data owners’ consent. Personal data sold by Ismentin comprises personal data he gathered from various sources such as financial institutions, car and property agents/vendors, and personal data from social media. He compiled the data and sold it. In brief, the court held that Mr. Ismentin had violated Article 32(2) of the EIT Law, which stipulates as follows:

“every person is prohibited from intentionally and without right in any way moving or transferring electronic information and/or electronic documents to other unauthorized party’s electronic system”.

Violation of such provision shall be subjected to a maximum imprisonment of nine years and/or a maximum fine of IDR3,000,000,000 (three billion Indonesian Rupiah). The interesting thing about this case is despite the absence of comprehensive personal data protection in Indonesia, the court was still able to find a way to penalize the unauthorized access of personal data. The provision relied upon by the court was not specifically formulated to tackle the concept of data protection, with no mention of “personal data” in this provision. Instead, it only prohibits the unauthorized transfer of

---

62 Note that there is no information available on how frequently similar cases have occurred.
63 Rahmansyah and Nabila (n 22).
64 Bandung District Court v Buni Yani [2017] Bandung District Court (Bandung District Court).
65 Rahmansyah and Nabila (n 22).
66 Tangerang District Court v Abi Warnadi Ismentin als Joe Titan [2019] Tangerang District Court, 372/Pid.Sus/2019/PN Tng (Tangerang District Court).
67 K&K Advocates, ‘Unauthorized Transfer of Personal Data Might Be Punishable Under the Indonesian Criminal Law’.
electronic information and/or electronic documents. However, as personal data is transferred in electronic form, it can be considered as electronic information. Therefore, the EIT Law may apply to this type of personal data. Note that in this law, any personal data obtained without securing the consent from the data subjects and satisfying the requirement under the EIT Law, GR 71/2019, and MoCI 20/2016, a transfer of personal data can be considered as “unauthorized”.  

The EIT Law allows any violation of the GR 71/2019 and MoCI 20/2016 to be resolved privately through a court trial, in accordance with the applicable laws and regulations. Generally, a court trial can be filed based on one of two grounds, a breach of contract or any unlawful act. Specifically, for unlawful acts, the plaintiff must prove that the defendant has committed an unlawful act contrary to the laws and regulations, causing a loss to the plaintiff. There must also be a causal link between the unlawful act and the losses suffered by the plaintiff.

There are no express provisions for class actions over data protection and/or cybersecurity violations, as are available under the Indonesian Environmental Law and Consumer Protection Law. It is unknown if there has ever been an attempt to file a class action suit for data protection and cybersecurity violations.

2.6 Interim Conclusion

In the Indonesian legal system, there is no single unified regulation concerning personal data protection as it is scattered across various sectoral regulations and not unified under one comprehensive regulation such as the EU GDPR. However, these sectoral regulations contain provisions that briefly discuss the level of data protection that might be needed in each sector, without any prior obligation to do so. Further, there is no dedicated national data protection authority that oversees personal data protection in Indonesia. However, the MoCI, along with Ditjen Aptika is responsible for ensuring compliance with the data protection regime of Indonesia. With regard to penalties, any violation of Indonesia’s main data protection regulations (for instance, collecting, processing, analyzing, storing, promoting, announcing, transmitting, or publishing any personal data without the right to do so; as well as altering, reducing, tampering, deleting, moving or hiding any electronic information or records, etc.) could trigger the MoCI, through Ditjen Aptika, to impose either administrative sanctions, criminal penalties, or might both. Each law will mostly only cover specific sectoral value and will not generally apply, though some are related to each other. In the context of enforcement, disputes are settled on a case-by-case basis since there is no threshold of the “loss” caused by a data breach and mostly involve either the EIT law or various criminal laws.

The scattered nature of privacy and data protection provisions in Indonesia causes the overlapping of authority during enforcement. This overlapping authority can lead to negative consequences, such as the misuse and abuse of the collection and intervention of personal data that can violate the rights of data subjects. The various sectoral regulations combined are not adequate due to their broad and unclear nature. As the regulations are scattered, there is no uniformity and harmonization of the concept of data protection. Furthermore, the implementation of such regulations is also debatable in the context of their enforcement, as some cases can be tackled and resolved through the existing privacy and data protection regulations and some that cannot and are solved through alternative ways. The absence of uniformity and harmonization on the concept of data protection can also affect the magnitude and duration of the criminal punishment towards the person that misused the personal data. This raises questions regarding the severity of criminal punishment imposed on the abuser of personal data. Looking back at the unauthorized data transfer case, Mr. Ismentin was not only punished by the provision as stated in the EIT Law but also by the criminal law. In the human rights context, I wonder whether this double punishment is fair for Mr. Ismentin, despite

68 ibid.
69 ibid.
the mistakes he has made. The problem here is not only the nature of punishment to be imposed on the violator or abuser but also determining the appropriate quantum of punishment that fits the illegal actions conducted. Hence, the formation of a new comprehensive and unified data protection regulation in Indonesia along the lines of the GDPR and the PDPA can pave the way for tackling the inconsistencies discussed such as overlapping authority, scattered nature of regulations, unauthorized transfers of data, and so on, arising due to the existing patchwork of laws regarding the Indonesian data protection regime.
CHAPTER 3 – THE CHALLENGES IN THE ENFORCEMENT OF INDONESIAN PRIVACY AND DATA PROTECTION LAWS

3.1 Introduction

Data protection regulations play an important role in today’s data-driven economy. Implementing a successful data protection regime has become a complex task, despite the existence of a comprehensive and detailed regulation like the EU’s GDPR. To name a few, the difficulties from such an implementation are, among others, from regulatory, institutional, and cultural perspectives. The lack of uniform data protection-based regulation in Indonesia poses different challenges.70

In Indonesia, the discussion of personal data protection has increased in the last two years, especially since Facebook revealed that the personal information of Indonesian Facebook users could have been collected and stored by Cambridge Analytica.71 72 Since then, Indonesian citizens have questioned the protection of their own personal data. Further, Indonesia is one of the ASEAN countries which lacks a unified and adequate data protection regime.73 74 This lack of data protection has led to the increase in cases involving the misuse of personal data, such as the disclosure of bank customers and credit card holders data,75 the divulgence of customers’ identity cards information for the debt collection process,76 along with the daily targeted text messages sent by individuals to offer various products and services like fast loans and credits.

While Indonesia is yet to enact a comprehensive data protection law, the amendment to GR 82/2012 has incorporated some measures pertaining to data protection. In brief, GR 82/2012 (as amended by GR 71/2019) regulates the ongoing use of regional operating platforms that have, to date, tended to host Indonesian data processing operations across various jurisdictions such as Singapore.77

Furthermore, with a population of over a quarter billion and one of the fastest-growing economies in the world, Indonesia is becoming an important player for multinational businesses. However, this

70 Putri (n 1).
71 To solve the case, the Indonesian government issued a warning letter to Facebook Indonesia, but no further actions were conducted to settle this matter. See https://www.thejakartapost.com/life/2018/04/06/facebook-faces-indonesian-police-investigation-over-data-breach.html.
72 Cambridge Analytica is a company that provides services to businesses and political parties who want to “change audience behavior”, where it claims to be able to analyze vast amounts of consumer data and combine that with behavioral science to identify people that can be targeted by the marketing material. It gathers data from a wide variety of sources, including social media platforms such as Facebook and its own polling.
73 Thio Tse Gan, ‘Data and Privacy Protection in ASEAN - What Does It Mean for Businesses in the Region?’
74 The development of data protection regulation in ASEAN has so far been uneven. Until recently, Singapore, Malaysia, and the Philippines were the only countries that have established unified personal data protection laws. The latest country in ASEAN that enacted data protection laws is Thailand. On the other hand, Indonesia has considered a general data protection law and had a draft queued in the legislative process. The remaining countries in ASEAN do not have overarching regulatory frameworks for data protection. However, there are laws in specific sectors or for electronic media that regulate personal data.
77 According to the temporary-person-in-charge of Ditjen Aptika (Anthonius Malau) in 2019, GR 82/2012 is considered to be no longer compatible with the current development of Indonesian citizens’ legal needs. Therefore, an amendment needs to be issued by the government. See https://cyberthreat.id/read/3608/Kominfo-PP-71-Tak-Berbenturan-dengan-Kedaulatan-Data.
78 There are some notable provisions on GR 71/2019 that includes more extensive provisions such as: (1) a new concept of Public and Private ESP; (2) new data localization requirements for Public ESP; (3) further elaboration on the deletion of electronic data; (4) provisions on electronic certificates and electronic reliability certificates; and (5) a new scope of electronic certification services.
issue poses a challenge to foreign players that are willing to invest in Indonesia, especially in the field of technology.79

With regard to the challenges faced in enforcing the current privacy and data protection law and regulations in Indonesia, based on my research, there are three main challenges, namely: (1) Regulatory challenges, (2) Institutional challenges, and (3) Cultural challenges. To provide a further understanding of these challenges, they will be elaborated on in the upcoming sub-sections.

### 3.2 Regulatory Challenges

Despite the current data protection regime being scattered across 30 regulations, there are only three important regulations that are commonly referred to when discussing personal data protection in Indonesia, namely: The EIT Law, GR 71/2019, and MoCI 20/2016. However, please note that the other regulations can also be used in dealing with privacy and data protection matters, depending on the context, as again, Indonesia does not have a unified and comprehensive data protection law.

In order to provide a clearer picture related to the abovementioned regulations in Indonesia, the following table summarizes the content of these laws:

<table>
<thead>
<tr>
<th>Law/Regulation</th>
<th>Articles related to personal data</th>
<th>Scope or limitation of the regulation</th>
<th>Subject of the regulation and provision</th>
</tr>
</thead>
<tbody>
<tr>
<td>EIT Law</td>
<td>Article 26(1) “except otherwise regulated in another regulation, the use of information related to personal data in electronic media should be conducted based on consent”</td>
<td>Processing, transmission, and sharing/transfer of personal data through an electronic system</td>
<td>Individuals and companies</td>
</tr>
<tr>
<td>GR 82/2012 (as amended by GR 71/2019)</td>
<td>Article 1(29) “personal data is any data on a person which is identified and/or may be identified individually or combined with other information both directly and indirectly through an electronic system and non-electronic system”</td>
<td>Collection, management, and processing of personal data in electronic systems and non-electronic system</td>
<td>Individuals, state institutions, and companies</td>
</tr>
<tr>
<td>MoCI 20/2016</td>
<td>Article 1(1) “Personal Data are certain types of data that have their validity preserved, maintained, and safeguarded, as well as their confidentiality protected”</td>
<td>Acquisition, collection, processing, storage, display, announcement, transfer, sharing, and annihilation of personal data in electronic systems</td>
<td>Individual, state institutions, business entities, or civil society that operate and/or use electronic systems</td>
</tr>
</tbody>
</table>

---

“Certain Types of Personal Data is any valid and factual information that is inherent and identifiable either directly or indirectly, on each individual and that their utilization should conform with the provisions of laws and regulations.”

| “Certain Types of Personal Data is any valid and factual information that is inherent and identifiable either directly or indirectly, on each individual and that their utilization should conform with the provisions of laws and regulations.” |

Based on the above, Article 26 of the EIT Law specifically prohibits the use and transfer of personal data without the relevant individual’s consent. Furthermore, it also states that relevant individuals can file a complaint and request financial compensation if they can assume that their personal data has been transferred without their consent. Additionally, in the amendment of the law, ESPs are obligated to immediately revoke irrelevant electronic information or documents based on the data owner’s request through a court decision. However, it does not comprehensively discuss the definition and the scope of personal data.

As for GR 82/2012 (amended by GR 71/2019), this regulation specifies the obligation of ESPs, specifically, by regulating the use and location of the data center. Besides that, protecting personal data is an important obligation for the ESPs mandated by this regulation. Another obligation of the ESPs under this regulation is to notify users of personal data protection failures. However, as with the EIT Law, this regulation does not provide a clear definition and scope of personal data, making it difficult to assess which data processing operations it applies to.

Slightly different from the two regulations mentioned above, the MoCI 20/2016 provides a more detailed definition of personal data. Interestingly, there are two definitions regarding personal data defined in this regulation. As mentioned in the table above, the first definition concerns the personal data itself, where it is defined as “certain types of personal data that have their validity preserved, maintained, and safeguarded, as well as their confidentiality protected.” The second definition concerns certain types of personal data (data perseorangan tertentu), where it is defined as “any valid and factual information that is inherent and identifiable, either directly or indirectly, on each individual and that their utilization should conform with the provisions of laws and regulations.”

The difference between both definitions is that the first definition regarding personal data is more general than the second definition. The second definition further elaborates on the “certain types of personal data” as mentioned in the first definition. Further, the personal data subjects’ rights are also laid down in the regulation, even though they are not comprehensively stipulated.

To summarize, the above three regulations only focus on personal data that is processed through electronic systems. In contrast, the non-electronic means of personal data collection, processing, and use are still governed by the sectoral regulations elaborated in Chapter 2 and Annex 1. For example, the collection, processing, and transmission of personal data in the financial sector are specifically addressed in OJK Regulation No. 77/POJK.01/2016 on Information Technology-Based Lending Services and OJK Regulation No. 13/POJK.02/2018 on Digital Financial Innovation. The abovementioned regulations do not refer to MoCI 20/2016 and have their own subject and scope.

---

80 Law No. 19 of 2016 on Amendment of Law No. 11 of 2008 on Electronic Information and Transactions.
81 According to Article 26 of MoCI 20/2016, The rights of the personal data subject are as follows: (1) the right to the secrecy of their personal data; (2) the right to file a complaint to the MoCI in case of any personal data dispute settlements due to the failure in protecting the confidentiality of their personal data; (3) the right to access or rectify their personal data without disrupting the personal data management system; (4) the right to access the history if their personal data have been submitted to the ESPs as long as it is still in accordance with the applicable regulations; and (5) the right to erasure of their personal data unless specified otherwise in the Indonesian laws and regulations.
The MoCI 20/2016 limits the retention period of personal data to five years minimum. In government institutions, archiving and retention of data, including personal data, is regulated by Archival Law, while the business sector usually has its own policy on the data retention period. In terms of data transfer and sharing, the abovementioned regulations rely on written consent that should be provided in the Indonesian language, but there is no further provision regarding the procedure to obtain such consent.

Even though the MoCI 20/2016 provides more details on personal data protection, the regulation level is still insufficient to be impactfully enforced. Ministerial regulations only allow the imposition of administrative sanctions in terms of data protection misuse. The EIT Law has strong sanctions for the misuse of electronic information. However, it does not have a clear definition of personal data making it difficult to obtain sufficient evidence to bring a case before the relevant court.\(^\text{82}\)

The insufficient level of ministerial regulation also makes it difficult to expect good enforcement as mandated by the regulation. The government institutions are still adhering to their sectoral laws rather than the MoCI 20/2016. The business sector also prefers to refer to the GDPR and PDPA as the main sources for developing their data protection policies.\(^\text{83}\)

Based on the above elaboration, the regulatory challenge is evident and can be seen from the insufficiency of the existing data protection regulation in providing comprehensive protection to Indonesian citizens. One of the significant examples is that the existing regulations focus more on the obligation of ESPs that collect, process, and use personal data. It lacks the details of data subjects’ rights and the person responsible for protecting these rights.

### 3.3 Institutional Challenge and Accountability Process

Based on my research, there are two main institutional challenges within the government that have been observed during the implementation of the current data protection regime in Indonesia:\(^\text{84}\)

1) Overlapping responsibilities:

   Currently, there is no designated data protection authority responsible for supervising the protection of personal data in Indonesia. As such, disputes are still being handled by ministries or independent agencies that have been mandated to be in charge of their respective fields. For instance, the Ditjen Aptika will be responsible for any breach of personal data conducted by the ESPs, while the OJK shall be responsible for the breach within the scope of the financial sector, as well as the Ministry of Health that is responsible for the breach related to medical records and other issues in the health sectors.

2) Lack of knowledge, capacities, and capabilities of regulators:

   Most state officials are still not aware that they are processing someone’s personal data, and there is no specific law or regulation, as well as internal policies that elaborate how to process someone’s personal data in detail, e.g., how to obtain the consent of data subjects while processing their personal data. Furthermore, as the existing regulations focus mostly on ESPs, the state officials still feel that the regulations do not bind them, although it is clearly stated in MoCI 20/2016, it applies to state officials if they process personal data in an electronic system.

---


\(^{83}\) Putri (n 1).

\(^{84}\) Ibid.
Furthermore, the MoCI also encourages “capacity-building” programs with regards to data protection, where the MoCI regularly sends state officials from different institutions to participate in workshops, training, and certification programs related to data protection. Even though there are attempts to improve state officials’ capacity and knowledge, they are very limited.

The business sector has more advanced institutional capacities. Based on an interview conducted between the World Wide Web Foundation and relevant companies, three out of four company interviewees confirmed that they already have a dedicated officer to handle personal data protection related matters\(^85\), who is usually employed under the Legal and Compliance Department, or with the IT Department. Besides that, all companies interviewed also had some kind of internal “capacity-building” programs (similar to the ones provided by the MoCI) to improve the officers’ knowledge and capability in data governance and personal data protection. Some business associations have also created guidelines for personal data protection. One example is the Indonesian Fintech Lender Association/Asosiasi Fintech Pendanaan Bersama Indonesia (AFPI), which created guidelines discussing the obligation to obey and implement the existing regulation on personal data protection related matters in each company, and the eligible debt collection procedure for online lending companies.\(^86\)

Accountability issues are also a part of the institutional challenge. The weak sanctions, the absence of an independent investigator, and the unclear and overlap of authorities in handling personal data misuse because of ununified regulations lead to a toothless accountability process. For now, the reports of personal data misuse are mostly being received by the MoCI, but they do not have the authority to impose sanctions and only act as an intermediary. The MoCI forwards cases to the Attorney Office of Indonesia (for personal data cases related to defamation) or to the relevant sectoral ministry, such as OJK, in the financial sector. Based on the interview conducted between the World Wide Web Foundation and relevant human rights organizations, state officials, and representatives of the business sector, they agree that there is always insufficient evidence/prooﬁ to process a lawsuit related to the misuse of personal data.\(^87\)

Besides that, there is no procedure in the current data protection regime to ensure transparency and accountability in the context of personal data processing. Since the regulations that have been elaborated in this chapter and in the previous chapter do not detail any mechanism to counteract personal data misuse conducted by the government, the accountability process of how personal data is stored, who has access to it, and the mechanisms for data sharing, are never disclosed.\(^88\)

### 3.4 Social and Cultural Challenges

Indonesian citizens are the most vulnerable actors in the absence of a unified and comprehensive data protection regulation in Indonesia. However, most citizens are still not familiar with the basic concepts such as privacy and personal data protection. In Indonesia, personal data is yet to be part of important information and therefore is not consciously protected. This lack of awareness relates closely to the cultural background that has long been studied as a crucial part of the regulatory privacy mechanism.\(^89\) Based on this fact, the country has not accounted for its citizens’ cultural characteristics in constructing and implementing relevant regulations.

\(^{85}\) ibid.  
\(^{86}\) ibid.  
\(^{87}\) ibid.  
\(^{88}\) ibid.  
\(^{89}\) Sabine Trepte and others, ‘A Cross-Cultural Perspective on the Privacy Calculus’ (2017) 3 Social Media and Society.
Discussing privacy and personal data with the Indonesian citizens is quite tough, as most still perceive privacy not as a human right but more as a “security”. There is a fear of going back to the “New Order” era (when Indonesia was led by Soeharto, the second president of Indonesia), where everything was closed and protected by the government. Most Indonesian citizens fear that the government will close the information that is now open to the public. Furthermore, looking at the Indonesian citizens’ general online behavior, only a small percentage is aware of the risk of privacy and personal data misuse. In contrast, most citizens neglect the risk of privacy and personal data misuse to acquire benefits from the services they use online, especially if it is free. For example, the risk of privacy intrusion in the online lending application is often neglected, especially by female users, due to benefits such as applying for credit loans without their spouse’s approval. Similarly, they also neglect the risk of personal data misuse by the provider of the application or the loan provider. They do not really care that there is a possibility that their personal data can be misused by the provider of the application or the provider of the loan through the practice of direct sale and purchase of their data.

Despite many cases and stories concerning privacy and personal data intrusion in Indonesian news, it is still an unfamiliar issue. I am of the view that there is an urgent need to spread awareness regarding the importance of securing personal data in different ways, such as educational systems and business practices. The government institutions should not neglect their important role in providing comprehensive protection to citizens for such issues.

Based on my research from the literature and news, as well as people that have been interviewed by the World Wide Web Foundation, there is an expectation of the future data protection law or regulation to not only construct a regulation but also educate its citizens regarding the importance of securing their own personal data. However, since the most comprehensive regulation available now is the GDPR, most aspects of the Indonesian data protection regulation draft refer to the GDPR.

Due to the differences in cultural characteristics, referring to the GDPR is not always the best option. For example, the GDPR has advanced articles on privacy and data protection, focusing on the obligation of data processors and controllers. This is because European citizens have different levels of understanding of the concept of data protection. Further, in the EU, the directives on data protection have been issued since 1995. In this regard, the EU citizens have had plenty of time to understand the concept of data protection, especially in the lead up to when the GDPR was discussed in 2014 and enforced in 2018. Since the enactment of the GDPR, the EU has tried to spread awareness regarding the concept of data protection by attributing a total of EUR5 million to 19 projects aiming at supporting the implementation of the GDPR. However, even though the EU citizens have had a lot of time in experiencing and understanding deeper the concept of privacy and data protection, this

---

90 Putri (n 1).
91 ibid.
93 Putri (n 1).
94 Trepte and others (n 89).
95 Earlier on, in 2017-2018, the EU has granted EUR2 million to six projects for raising awareness of data protection in Europe. Amongst other: (1) the Stitching European Lawyers Foundation that organized training of lawyers on the EU data protection reform; and (2) the Law and Internet Foundation trained local public authorities for the new data Protection Legislation in Austria, Bulgaria, Greece, Latvia, Romania, and Slovakia. Subsequently, some other activities organized by the EU’s data protection authorities are as follows: (1) A Privacy and GDPR awareness campaign has been held for Belgium’s citizens; (2) An awareness-raising seminar has been held for Latvian Small and medium-sized enterprises and minors; and (3) An awareness-raising seminar regarding data protection in the Netherlands, and more particularly raising the profile of the Dutch DPA. See https://ec.europa.eu/info/law/law-topic/data-protection/eu-data-protection-rules/eu-funding-supporting-implementation-gdpr_en.
time gap does not guarantee that they have better privacy and data protection awareness, as the efforts to maintain privacy and data protection awareness have been going on since before the GDPR was enforced.96

Indonesia is still struggling to juggle between educating citizens on privacy and data protection, constructing a comprehensive legal framework on personal data protection, and maintaining its growing digital economy. Additionally, besides referring to the GDPR, referring to the practices from neighboring countries that already have a data protection legal framework, such as the Philippines and Singapore, might be useful considering the similar income level and industrialization to Indonesia.97

3.5 Recommendations and Measures that can be adopted by Indonesian Government

Personal data protection is one way of protecting the right to privacy as a basic human right. Even though Indonesia does not have any single unified regulation which regulates personal data protection, the protection guarantee of the right to privacy is contained in the Indonesian Constitution, as emphasized in Article 28(G)(1):

“Every person shall have the right to protection of his/herself, family, honor, dignity, and property, and shall have the right to feel secure against and receive protection from the threat or fear to do or not do something that is a human right”

The affirmation of a similar statement is also stipulated in Article 29 HAM Law. Unfortunately, such constitutional guarantees have not been well implemented within the right level of legislation. It seems like the majority of the public in Indonesia has not made personal data as a part of their human rights that need to be protected. Therefore, it is very common to find people who unconsciously waive their right to privacy or personal data carelessly, just to obtain certain benefits, as discussed earlier in the sub-chapter 3.4.98

Responding to large-scale data collection practices that collect various types of data for various interests, it is urgent for the Indonesian government to prepare a robust data protection regulation for Indonesian citizens. Based on my research, I believe the following suggestions must be adopted by the Indonesian government:99

1) Clear guidelines on data collection and processing should be implemented even in the absence of a unified and comprehensive regulation on data protection. A stiff legal framework might be less useful considering the lack of understanding of Indonesian citizens regarding privacy and data protection and the readiness level of stakeholders that will be affected. Therefore, providing some guidelines on the protection, collection, and processing of personal data will be more useful. The abovementioned guidelines can be used by government institutions or big companies and micro-small enterprises, start-up companies, civil society organizations, and citizens at large. Further, in the future, clear guidelines on data collection and processing will not be enough. Therefore, an initiative to have a deep discussion on a data protection law or regulation is also needed.

2) Due to ingrained sectoral work among government institutions and a lot of collection and processing of personal data (by government institutions and the private sector), a single-independent body/agency responsible for data protection is required. The body/agency model should be discussed further, considering various factors such as the functionality, structure, and the state budget available to establish such an agency. Alternatively, this

---

96 Putri (n 1).
97 ibid.
98 Djafar (n 2).
99 ibid.
independent agency could be suggested through parliament as one of the future data protection law or regulation pillars. The establishment process of this body should be transparent and closely monitored by all relevant stakeholders.\(^{100}\)

3) With regard to the type of sanctions, if administrative sanctions\(^{101}\) are not working really well, a gradation of financial sanctions could be an option. The gradation might be based on (1) the nature of the legal subject (i.e., individual or organization); (2) the size of enterprise, company, or organization; and/or (3) the quantity of personal data that is processed. Furthermore, there should be a clear remedy mechanism for the victims of the misuse of personal data.

4) A regulatory sandbox model – a mechanism where regulation is developed in parallel with the change of business models and innovation to be implemented for future data protection law or regulation. The discussion that has been ongoing in the bill drafting process by the stakeholders could be continued as a sandbox. Other important actors can be added along the way if necessary. The advantage of this practice is that it can tackle two main uncertainties at the same time: the uncertainty of growing digital innovation and the uncertainty of the regulations themselves.\(^{102}\) It could become a new learning process for the enforcement of the current law and the establishment of future law whilst maintaining the growth of an innovative digital ecosystem.\(^{103}\)

5) Strengthening and harmonizing Indonesian citizens’ movement on privacy and personal data literacy from the grassroots level, which could add a cultural dimension in the implementation of data protection regulation and could become a solution to tackle the gap of privacy culture and knowledge among Indonesian citizens. The addition of a cultural dimension in the construction and implementation of the regulation is important to make Indonesian citizens more culture-sensitive with regard to the concepts of privacy and personal data.

3.6 **Interim Conclusion**

This chapter discussed three main challenges in implementing the regulation on the data protection regime in Indonesia. First, regulatory challenges were addressed. It has been confirmed that the existing regulation, even though there are many regulations in Indonesia that recognize privacy and data protection as a concept, is still insufficient in providing comprehensive protection to Indonesian citizens. The target groups for the existing regulations are also quite specific, with more articles and procedures/mechanisms specifically defined only for ESPs. There are obscure and ambiguous notions for individuals and the public sector as legal subjects that create an unclear understanding among stakeholders. Despite these uncomprehensive regulations, in the business sectors, especially big companies, including ESPs, are having their own policies related to data protection. In this regard, they are referring to the European GDPR or the Singaporean PDPA as these two are the world’s most comprehensive data protection laws.

The second challenge is the institutional challenge. Apparently, from the elaboration above, government officials and law enforcers seem to lack awareness of how to interpret the existing regulations. There is no single regulator for data protection available in Indonesia. Various government institutions also handle the settlement of alleged data breach and misuse cases. As the

\(^{100}\) Ibid.

\(^{101}\) According to Article 36(1) of MoCI 20/2016, the administrative sanctions are as follows: (1) oral warning; (2) written warning; (3) temporary suspension of activities; and/or (4) online announcement through websites. While according to Article 100(2) of GR 71/2019, the administrative sanctions are as follows: (1) written reprimand; (2) administrative fine; temporary suspension; access termination; and/or removal from the list.

\(^{102}\) Elizabeth Denham, ‘Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice’ 1.

\(^{103}\) Putri (n 1).
citizens are not expected to be able to distinguish between processors and controllers or to directly check what is being done with their data (with regard to the different levels of understanding of the data protection concept), the country-level data protection authorities should mainly conduct the task of understanding the privacy concepts deeper. Besides, it is also not possible for individuals to do this effectively. Therefore, there is an urgent need to establish detailed information regarding a single data protection authority and data protection officer in the future data protection law.

The third is a cultural challenge. In general, Indonesian citizens do not consider privacy and personal data security/safety as an inherent part of their citizens' rights. Therefore, only a small amount of personal data misuse and breaches are reported, although citizens know that their data is being traded massively. The existing data protection regulations are not being communicated entirely. This makes it really difficult for Indonesian citizens to understand the importance of securing their own personal data and how they can benefit from securing it. Apparently, there is an importunate need to spread, disseminate, and increase the awareness and understanding of the importance of securing personal data to Indonesian citizens. It is recommended for the government, business sector, and civil society organizations to participate in this spreading process. Understanding the cultural background of a country is very important to construct better future data protection laws or regulations.

In this chapter, I have elaborated the challenges faced in enforcing the current personal data protection regime in Indonesia and the measures that can be adopted by the Indonesian government to address the challenges effectively. In order to understand how the Indonesian government should make a better data protection regime, in the next chapter, I will assess the legal framework that protects personal data in the EU and Singapore and provide an analysis of what lessons can be learned by Indonesian policymakers from the EU and Singapore’s experiences on personal data protection.
CHAPTER 4 – KEY ELEMENTS TO BE TAKEN INTO ACCOUNT BY THE INDONESIAN POLICYMAKERS IN REGARD TO THE NEED OF A UNIFIED PRIVACY AND DATA PROTECTION LAW

4.1 Introduction

This chapter aims to evaluate the legal frameworks which protect personal data in the EU and Singapore, beginning with a brief historical background of the EU’s GDPR accompanied with a discussion on the objectives and goals, notable provisions, data protection institutions in the EU, penalties, and enforcement. After this, Section 4.3 will contain a similar discussion on the Singapore PDPA. The relevant provisions of both regulations are discussed and selected, considering the major drawbacks of Indonesian data protection law highlighted in Chapter 3. Furthermore, Section 4.4 contains the analysis of the lessons which can be learned by Indonesian policymakers from the EU and Singapore’s experiences on personal data protection.

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

In the EU, personal data protection law was first harmonized in 1995 by the Data Protection Directive 95/46/EC (1995 Directive). However, as a directive, it was not directly applicable to the EU member states and had to be transposed into national laws, resulting in a framework comprising of 28 similar, but different, national laws of the various EU member states. More than 20 years later, the new General Data Protection Regulation (GDPR) aims at harmonizing the data protection laws of the EU by creating a single set of rules that is directly applicable to the Member States as a regulation. The GDPR also provides further details and adds new elements towards the concepts, rights, and obligations set out under the 1995 Directive.

In terms of its objectives and goals, the GDPR expressly stipulates three objectives. The first is to harmonize the data protection laws of Europe, which is achieved through the GDPR’s regulatory framework and does not require member states to further transpose the GDPR into their own national legislation. Secondly, the GDPR calls for the protection of fundamental rights by protecting individual’s rights with respect to their personal data, by establishing a set of principles and rules for safeguarding data processing activities involving the personal data of individuals. The third objective of the GDPR is to ensure the free movement of data and is embodied in the economic rationale of the regulation, which acknowledges that the functioning of the European internal market requires the free movement of data.

The above aims are realized by several key provisions of the GDPR. For example, the principles of data protection listed in Article 5 of the GDPR must be complied with while performing any data processing activity – thus ensuring a high standard of protection of the rights of citizens. The principles are listed as follows: (i) lawfulness, fairness, and transparency; (ii) purpose limitation; (iii) data minimization; (iv) accuracy; (v) storage limitation; (vi) integrity and confidentiality; and (vii)

---

105 ibid.
106 Article 1 of 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).
107 Article 1(1) of the GDPR.
108 Article 288 of Treaty of Functioning of the European Union (TFEU), consolidated versions of TFEU 2012/C 326/01. The regulatory form of regulation provides maximum harmonization across the EU. Further, according to Recital 8 of the GDPR, in the event of the GDPR allow member states for specifications or restriction of rules set forth in the GDPR through national law, member states may only do so as far as necessary for coherence and for making national law comprehensible.
109 Article 1(2) of the GDPR.
110 Recital 2 of the GDPR.
111 Article 1(3) as well as Recital 2, Recital 6, Recital 7, and Recital 13 of the GDPR.
112 Recital 13 of the GDPR.
accountability.\textsuperscript{113} Beside the abovementioned principles, the lawfulness of processing as stated in the Article 6 of the GDPR is also considered as a key provision in the GDPR, where any data processing can only be considered as lawful only if at least one of the following applies: (i) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (ii) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering to a contract; (iii) processing is necessary for compliance with a legal obligation to which the controller is subject; (iv) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (v) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or (vi) processing is necessary for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.\textsuperscript{114} With regard to the consent, Article 7 of the GDPR also elaborates that consent and its conditions as a ground for processing personal data to establish a safer online data processing environment.\textsuperscript{115} It is clear from the GDPR that lawful consent for personal data processing must be provided in the form of a \textit{“clear affirmative act”}.\textsuperscript{116} Furthermore, the grounds for consent to be regarded as valid as listed in Article 7 set a considerably high threshold in order to protect individuals from unlawful use of their personal data.\textsuperscript{117}

Therefore, based on the abovementioned key provisions in the GDPR, some of the implications, without being exhaustive, are as follows: (1) it encourages companies to carefully evaluate procedures for the processing of data; (2) it facilitates data protection by obligating companies that use personal data to vet service providers and impose contractual limits on data use; (3) the GDPR sets a high standard on the definition of lawful consent, on par with consent involving fundamental rights in other instances, e.g., for medical treatment; and (4) the GDPR also emboldens firms to develop information governance frameworks, to in-house data use, and to keep humans in the loop in making the decision.\textsuperscript{118} \textsuperscript{119} It has higher standards, stricter laws, and tougher sanctions than the 1995 Directive.

In accordance with the GDPR, member states now have designated national data protection authorities/ supervisory authority (DPA) to ensure the protection of their citizens’ personal data.\textsuperscript{120} The DPA’s have the investigative, corrective, authorization, and advisory powers.\textsuperscript{121} The DPA’s can commence on-site data protection audits, issue questionnaires, and also possess the power to issue public warnings, reprimands, and impose sanctions and fines for GDPR violations.\textsuperscript{122} At the Union level, the European Data Protection Board (EDPB), serves as a central data protection authority. Its duties are to monitor, supervise, and solve conflicts between national DPA’s and provide guidance.\textsuperscript{123}

The DPAs must determine the value of fines to be imposed for specific data protection violations based on the GDPR. These are applied as an additional penalty or as a substitute for further

\textsuperscript{113} Article 5(1) and (2) of the GDPR.
\textsuperscript{114} Article 6(1) of the GDPR.
\textsuperscript{116} Article 1(11) in conjunction with Recital 32 of the GDPR.
\textsuperscript{117} Article 7 of the GDPR. For consent to be valid and lawful: (i) the controller must be able to demonstrate that data subjects had consented; (ii) its collection must be distinguishable from other matters; (iii) can be withdrawn at any time; and (iv) utmost account must be taken when assessing the element of “freely given”.
\textsuperscript{118} \textit{Ibid}
\textsuperscript{119} Hoofnagle, Sloat and Borgesius (n 17).
\textsuperscript{120} Article 8(3) of the Charter of Fundamental Rights of the European Union 2012/C 326/02 (the Charter).
\textsuperscript{121} Article 57 and 58 of the GDPR.
\textsuperscript{122} DLA Piper, ‘DATA PROTECTION LAWS OF THE WORLD - Full Handbook’.
\textsuperscript{123} Crowell & Moring (n 103).
remedies or corrective powers, such as the order to end a breach or violation, an instruction for the data processor or controller to comply with the GDPR, or impose a ban on data processing altogether. The highest fines are of up to European Monetary Unit (EUR) 20 million or in the case of an undertaking up to 4% of the total worldwide turnover of the preceding year, whichever is higher and apply to a breach of: (1) the basic principles for processing including conditions for consent; (2) data subjects’ rights; (3) international transfer restrictions; (4) any obligations imposed by member state law for special cases such as processing employee data; and (5) certain orders of a DPA. The lower category of fines of up to EUR10 million or in the case of an undertaking up to 2% of the total worldwide turnover of the preceding year, whichever is higher, apply to the breach of: (1) obligations of controllers and processors, including security and data breach notification obligations; (2) obligations of certification bodies; and (3) obligations of a monitoring body.

According to statistics provided by the EDPB, there have been 281,088 cases logged by the various DPA’s within a year of the GDPR coming into force. Of these, 144,376 pertained to consumer complaints, and 89,271 pertained to data breach notifications by data controllers. The Netherlands, Germany, and the United Kingdom (UK) reported the highest number of breaches. Yet, according to the DLA Piper law firm’s “GDPR Data Breach survey” released in February 2019, just 91 GDPR fines have been handed out across the European Economic Area within the first eight months of the regulation coming into force. The figure has now risen but not by much, say experts. The EDPB’s February 2019 report to the European Parliament indicated that 11 countries had imposed GDPR fines totaling approximately EUR56 million.

Looking specifically at the GDPR enforcement and implementation in the EU, the following examples have been cited to show the effectiveness of the sanctions and enforcement of the GDPR itself. In the Netherlands, the Dutch DPA has effectively facilitated GDPR awareness by providing information, guidelines, and tools about its website’s regulation. As an example, the Dutch Credit Registration Bureau/Bureau Krediet Registration (BKR) was fined EUR830,000 by the Dutch DPA for violating data subject rights by its practice of charging fees and discouraging individuals who wanted to access their personal data. In Germany, on the other hand, the DPAs are organized on a state level, resulting in a total of 16 data regulators, which have collectively issued 75 fines since the implementation of the GDPR, totaling just EUR449,000 - issuing the largest fine of EUR80,000 towards a healthcare organization that exposed sensitive personal data. In the UK, the two biggest enforcement actions so far stemming from GDPR violations have come from the UK’s Information Commissioner’s Office, which has fined British Airways Great British Pound (GBP)183.4 million and Marriott GBP99.2 million for data breach-related violations.

---

124 Article 83(5) of the GDPR.
125 Article 83(4) of the GDPR.
127 ibid.
130 Hodge (n 125).
4.3 The Personal Data Protection Act 2012 (PDPA) (Regulation No. 26 of 2012)

The PDPA was enacted on 20th November 2012 and entered into force on 2nd July 2014 and is considered an important element of Singapore’s technology law framework. In general, it establishes comprehensive baseline standards and requirements for the protection of personal data. It also fills the gap in Singapore’s data protection regime, having previously only comprised of sector-specific regulations like Indonesia. In the development of this law, the Singapore government has taken inspiration from the data protection regimes of the EU, UK, Canada, Hong Kong, Australia, New Zealand, the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and the APEC Privacy Framework.

The PDPA regulates the collection, use, and disclosure of individuals’ personal data by organizations in a manner that recognizes both the right of individuals to protect their personal data and the need of organizations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances. It contains two main sets of provisions, covering data protection and the DNC registry, which organizations must comply with.

The PDPA seeks to promote three main objectives: (1) to give individuals the right to data protection in a balanced manner that does not impose overly onerous compliance costs on private organizations; (2) to recognize the qualified right of private organizations to collect, use, and disclose personal data to build up its position as a trusted business hub; and (3) to develop Singapore into a global hub by ensuring that Singapore is equal to the countries that have data protection laws so as to facilitate cross-border data transfers.

Content-wise, the PDPA shares many of the GDPR’s key provisions. For instance, referring to principles of data protection as listed in Article 5 of the GDPR, the PDPA listed what they called as an “obligation” in several separate articles, which are as follows: (i) the consent obligation; (ii) the purpose limitation obligation; (iii) the notification obligation; (iv) the access and correction obligations; (v) the accuracy obligation; (vi) the protection obligation; (vii) the retention limitation obligation; (viii) the transfer limitation obligation; and (ix) the accountability obligation. Further, Article 6 of the GDPR explicitly states the legal grounds prior to the data processing. In this regard, the PDPA does not explicitly outline legal bases for personal data processing. Under Section 13 of the PDPA, an organization cannot collect, use, or disclose personal data regarding an individual unless the individual gives, or is deemed to have given, his/her consent to the collection, and use.

133 Note that the existing sector-specific legislation and regulations will continue to apply as the PDPA was devised to be a complementary Act. Section 4(6)(b) states that “the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law”.
135 Personal Data Protection Commission - Singapore (n 19).
136 Chik and Pang (n 131).
137 Section 13 to 17 of the PDPA.
138 Section 18 of the PDPA.
139 Section 20 of the PDPA.
140 Sections 21 and 22 of the PDPA.
141 Section 23 of the PDPA.
142 Section 24 of the PDPA.
143 Section 25 of the PDPA.
144 Section 26 of the PDPA.
145 Sections 11 and 12 of the PDPA.
use, or disclosure.\textsuperscript{146} 147 On a separate note, it does provide that the collection, use, or disclosure can be done without the consent of the individual only if it is required or authorized under the PDPA or any other written law.

To provide a clearer picture of how the PDPA is supervised and enforced in order to show the effectiveness of the sanctions and enforcement of the PDPA, the following are the mechanism details on how the data protection regime in Singapore is implemented. The enforcement of the PDPA is supervised by the Personal Data Protection Commission (PDPC) of Singapore, which has the following powers and functions: (1) Investigative powers, powers of review (e.g., the issuance of rectification orders), and powers of enforcement; (2) PDPC provides guidance and auditing services for organizations, issues guidelines, and advisories on data protection concepts such as consent, reasonableness, and necessity; and (3) PDPC undertakes initiatives to spread awareness on personal data protection and privacy (e.g., through training sessions and guidelines that are customized for different industries).\textsuperscript{148}

The PDPA imposes fines and prison sentences as penalties for its violation. The amount of fine/prison sentence levied vary and depended on the relevant provisions that are breached.\textsuperscript{149} For example, obtaining unauthorized access or unlawfully modifying citizens’ personal data may either result in a fine not exceeding SGD5,000 (approximately EUR3,300) or imprisonment for a term not exceeding 12 months, or both.\textsuperscript{150} Further, organizations can be fined up to Singapore Dollar (SGD)100,000 (approximately EUR66,000), whereas individuals can be imprisoned and fined up to SGD10,000 (approximately EUR6,600) if they breach the PDPC throughout performing their duties and enforcement powers.\textsuperscript{151}

The enforcement of the PDPA in Singapore is supervised by the PDPC.\textsuperscript{152} Disputes can be resolved through civil lawsuits for private matters\textsuperscript{153} criminal prosecution for offenses committed under the PDPA\textsuperscript{154}, or alternative dispute resolution.\textsuperscript{155} As of 20 June 2019, the PDPC issued a total of 90 orders against 114 organizations for breaching the PDPA. The most common types of data breaches involve the deliberate disclosure of personal data, poor data security arrangements, errors in a mass email and/or post, and insufficient internal data protection policies.\textsuperscript{156} Within the 90 orders that have been issued by the PDPC, the following are some of the data breach cases with the highest and largest fines ever imposed by the PDPC to reflect the effectiveness of the sanctions and enforcement of the PDPA itself. Up until today, the highest fines that the PDPC has imposed on organizations are SGD250,000 (approximately EUR166,260) and SGD750,000 (approximately EUR498,790) respectively on SingHealth Services Pte Ltd and Integrated Health Information Systems Pte Ltd, for breaching their data protection obligations under the PDPA, where the data breach arose from a cyber-attack on SingHealth’s patient database system and caused the

\textsuperscript{146} Section 13 of the PDPA.
\textsuperscript{147} Under the PDPA, an individual has not given consent unless the individual has been notified of the purposes for which his/her personal data will be collected, used, or disclosed, and the individual has provided his consent for those purposes.
\textsuperscript{150} Part X of the PDPA.
\textsuperscript{151} Chik (n 147).
\textsuperscript{152} Section 29 and 30 of the PDPA.
\textsuperscript{153} Section 32 of the PDPA.
\textsuperscript{154} Chik (n 147).
\textsuperscript{155} Lim and Lee (n 126).
personal data of around 1.5 million patients to be compromised.\textsuperscript{157} Besides the above, PDPC has also imposed a mix of behavioral remedies combined with financial penalties.

For example, in December 2018, the PDPC issued a fine of SGD20,000 to WTS Automotive Services Pte Ltd for failing to make reasonable security arrangements to prevent the unauthorized disclosure of its customers’ personal data. In the first half of 2019, PDPC issued a fine of SGD16,000 to GrabCar Pte Ltd for failing to put in place reasonable security arrangements to protect the personal data of its customers from unauthorized disclosure (e.g., the customer’s personal data was disclosed to one other customer via an email sent out by GrabCar Pte Ltd. Further, on the same period, PDPC issued a fine of SGD8,000 for Matthew Chiong Partnership due to the failure to fulfill its protection obligation and openness/transparency obligation under the PDPA. PDPC also directed Matthew Chiong Partnership to place a data protection policy to comply with the provisions of the PDPA.\textsuperscript{158}

If we compare both the GDPR and the PDPA, it is noticeable that there is a difference in the possible imposition of significant monetary penalties in cases of non-compliance with each regulation. The GDPR’s maximum limit for monetary penalties is much higher than that of the PDPA. Based on my understanding, in the EU, the DPAs may develop guidelines that establish further criteria to calculate the monetary penalty amount, whereas, in Singapore, the PDPA does not include a similar provision as owned by the GDPR. However, the PDPC’s Guide on Active Enforcement states that even though the financial penalties are warranted, such penalties are reserved only for breaches, which the PDPC views as particularly serious in nature.\textsuperscript{159} In this regard, I am of the view that the PDPC is somehow “limited” by the abovementioned concern that might cause the gap or difference in the amount of fines imposed under the GDPR and the PDPA. Another notable point is that Singapore’s data protection enforcement is not designed to apply to the government, where it is more oriented towards commercial and economic development. In contrary to the GDPR where it does aim for both government and the public sector as well.

4.4 Lesson that can be learned from the EU and Singapore

From the above discussion on the GDPR and the PDPA, it is evident that these regulations provide an adequate level of protection to the data subjects. This is by virtue of the fact that both the legislations impose effective sanctions in scenarios wherein their provisions are violated. As a result, the companies that operate under the ambit of these regulations (the GDPR and the PDPA) tend to ensure that their processing activities are compliant with them. The author believes that the Indonesian policymakers should consider some important points of the GDPR and the PDPA as a reference for ensuring effective rights for the concerned data subjects because the GDPR and the PDPA are effective in terms of having mechanism and frameworks in place to enforce the regulation as well as it contains a comprehensive set of concepts and principles. Hence, the following are the lessons that can be taken into account from the above-mentioned legislations:

1) Harmonization of the current Indonesian regulations

As stated earlier, the EU’s personal data protection regime was reformed from the 1995 Directive into the GDPR. The reasons for the reform are varied. One of them is of a generic nature and has to do with the intrinsic rule-making desire to keep abreast of new technological advances so as to provide better and more efficient attainment of key public

\textsuperscript{157} See Re Singapore Health Services Pte Ltd and another [2019] SGPDPC 3.


\textsuperscript{159} Angela Potter and others, ‘GDPR v. Singapore’s PDPA Comparing Privacy Laws’ Comparing Privacy Laws: GDPR v. Singapore’s PDPA.
objectives in the new setting. As it is understood that next to the beneficial gain because of the establishment of new digital technologies, such technologies also brought along the unknown privacy risks that arose as the reality of collecting, processing, storing, and using data changed. In the EU, one particular problem has been the ease with which data can move across borders to other member states, which is understandable as, at that time, the EU has difficulty enforcing the data protection laws in foreign jurisdictions. It is also understandable as the 1995 Directive has to be implemented into national laws (which resulted in 28 similar, but different, national laws of the various EU member states). Further, even though both types of EU legal acts can, in principle, ensure a high level of harmonization across the member states, a regulation is directly applicable. It does not require additional domestic implementation (whereas a directive defines the results to be achieved, leaving the means for achieving them up to the member states). Additionally, regulations immediately become part of a national legal system, have a legal effect of national law, and override contrary national laws, not like the directive.

In brief, one of the reasons behind this harmonization is to overhaul the EU’s legal framework on the protection of personal data to further strengthen individual rights, especially in the face of challenges to those rights from globalization and new technologies, which caused a significant and comprehensive change from a Directive to a Regulation.

Indonesia is neither a union such as the EU nor a federal country like the United States of America. From the hierarchy perspective, the legislation in the form of laws and regulations (government regulation and sectoral/ministerial regulation) will apply nationally and directly to all Indonesian citizens.

As discussed in the earlier chapters of this thesis, Indonesia has no legal framework that can accommodate all data protection utilization activities and serve as the legal basis for collecting and processing the personal data of Indonesian citizens. The Indonesian government is currently only depending on regulations scattered across various sectors and three principal regulations elaborated earlier in chapter 3 of this thesis (i.e., The EIT Law, GR 71/2019, and MoCI 20/2016).

As previously discussed, many Indonesian scholars, privacy advocates, and research institutions have argued that the existing regulations are not adequate and sufficient as they are too broad and unclear and tend to overlap each other. As elaborated earlier, the overlapping can be seen from various aspects, where it overlaps in the sense that many regulations regulate the same concepts. I am of the view that the overlapping would not be an issue if those regulations still can provide comprehensive personal data protection without causing any confusion in enforcing it. Therefore, I am of the view that the Indonesian policymakers can learn from and adopt the concept of regulatory harmonization with respect to data protection regulation, similar to that of the EU.

In this regard, Indonesian policymakers could pass a new law or regulation to accommodate all of Indonesia’s data protection activities. This law or regulation could provide a unified and comprehensive framework (providing the base concepts, definitions, principles,

162 ibid.
163 Crowell & Moring (n 103).
164 Burri and Schär (n 160).
165 Chik (n 147).
166 Djafar (n 2).
This new data protection regulation should serve as the legal basis for all data processing related activities. The issuance of this new data protection regulation should not eliminate all of the existing principal and sectoral regulations currently used by the Indonesian government or interfere with its enforcement. Instead, the harmonization of these regulations is intended to strengthen the concept of personal data, which was previously reflected, but less comprehensive, in these existing principal and sectoral regulations. Therefore, I believe that this unified/harmonized data protection regulation will solve the overlapping problem and inadequateness in the existing sectoral regulations.

2) Mandatory designation of Data Protection Authority

As elaborated in sub-chapter 2.3 of this thesis, there is no specifically designated national data protection authority that oversees the protection of personal data in Indonesia. It is only the MoCI, through Ditjen Aptika, that is responsible for ensuring compliance with the data protection regime in Indonesia. Initially, the primary duties of the Ditjen Aptika were to formulate and implement the policy in the field of informatics. In carrying out its primary duties, Ditjen Aptika also performs the following functions: (1) formulating and implementing policies in the field of e-Government, e-Business, and information security, including improving information technology, and empowering informatics; (2) preparing the norms, standards, procedures/mechanisms, and criteria in the field of e-Government; (3) providing technical guidance and supervision in the field of e-Government; (4) performing evaluation and reporting in the field of e-Government, e-Business, and information security, including improving information technology, and empowering informatics; (5) conducting the administration in the Ditjen Aptika; and (6) carrying out any other tasks assigned by the Minister of Communications and Informatics.167

However, I am of the view that the MoCI and Ditjen Aptika cannot be considered as Indonesia’s designated data protection authority as their primary duty is not solely to supervise the protection of personal data in Indonesia but to regulate government affairs in the field of communication and information technology to assist the Indonesian president in administering the state.168 Further, the establishment of a specific authority (separate institution or government bodies) dealing with cases regarding data breaches would be a step in the right direction since it might ensure more excellent safety to data subjects with respect to the protection of their personal data. Also, it is critical to remember that the MoCI and Ditjen Aptika were not specifically designated to tackle issues regarding data breaches. At this juncture, even though the MoCI, through Ditjen Aptika, were delegated the authority to supervise and settle data protection disputes, their primary duty (as discussed earlier) is only to formulate and implement policies in the field of informatics. In light of this, it can be understood that their duties do not specifically focus revolving around data protection issues and thus are general in the context of data protection. Also, with regard to the development of data protection-related-breaches that have recently taken place in Indonesia, there are not many cases that have been resolved through court proceedings (several examples have been discussed in Chapter 2) and the fact that there are many cases that were not resolved through court proceedings. For instance, many online lending service providers in Indonesia have accessed and retrieved the data subjects’ personal information without securing their consent first. In this regard, the only punishment imposed on such service providers was a revocation of their licenses by the OJK.

---

In comparison with the activities of the DPAs in the EU and PDPC in Singapore, these institutions were established to specifically supervise the protection of personal data in each jurisdiction, where they were given the powers to carry out the supervision activity, resulting in better enforcement of the GDPR and PDPA. On the other hand, as elaborated above, the MoCI and Ditjen Aptika were not established to ensure Indonesian citizens’ data protection, which has resulted in weak and inadequate enforcement related to the data protection issues that exist nowadays in Indonesia. Therefore, establishing a dedicated national data protection authority with the same powers as given to the DPA and PDPC and being specifically mandated to supervise the data protection in Indonesia might also help reduce the data protection issues in Indonesia.

3) Mandatory designation of Data Protection Officer

Looking particularly at the practice that has already been developed within the EU landscape, most member states appoint Data Protection Officer (DPO) to ensure compliance with the GDPR. Article 39 of the GDPR regulates the tasks of DPOs as follows: (1) to inform and advise the organizations where the DPOs work in respect of those organizations’ obligations under the GDPR; (2) to monitor compliance (not just with laws and regulations, but also on internal policies on the protection of personal data). The GDPR explicitly states that compliance monitoring includes monitoring the delegation of responsibilities within the organization insofar related to data processing-related activities, awareness-raising and providing training to staff and performing audits; (3) to advise and monitor anytime the organization where the DPO work intends to carry out a data protection impact assessment (DPIA); and (4) to become the intermediary between the national data protection authority and the organization, particularly as a point of contact of the organization for matters related to the national data protection authority. The concept of DPO does not only exist in the EU but also in Singapore. In particular, the Singapore organizations are required to designate at least one individual to be a DPO to oversee the data protection responsibilities within the organization and ensure compliance with the PDPA. The function of the DPO in Singapore is quite similar to the one in the EU.

In light of the above, I am of the view that the Indonesian policymakers can adopt the DPO obligation mechanism from the EU and Singapore in the upcoming data protection law to boost its compliance. It means that the users of personal data will be required to employ a DPO within their organizations. The advantages of having the DPO within the organizations that process the personal data are: (1) from the users of personal data’s perspectives, having a DPO in their organization can help them monitor and assist their compliance with the data protection law. As additional advantages, it will also improve the way organizations protect and control personal data when they perform their respective data processing activities; and (2) from the data subjects’ perspectives. There will be more assurance for them as there

---

170 Article 39(1) of the GDPR.
171 Data protection impact assessments (DPIA) is somewhat an audit on any new or existing data processing operation carried out by a controller or processor in order to assess whether such operation is likely to result in a high risk to the protection of personal data of an individual.
is someone inside the organization that can ensure that the organization’s data processing activity is consistent with the applicable data protection law. Further, the DPO can also be the main point of contact in case the data subject has a request concerning personal data matters (e.g., request to access, rectify, or erase their personal data). With the DPO’s presence inside the organizations, they could “act” as an extension of the supervisory/governmental authority. With the data compliance task being taken care of, the supervisory/governmental authority will be able to focus on other tasks such as providing guidance, enforcement actions, adjudications, etc. Therefore, obliging to have a DPO in organizations that process personal data is one of many measures that can be learned and adopted by the Indonesian policymakers as it can ensure greater compliance, at least, from the organizations (data processor) side since DPOs are generally responsible for formulating an organization’s data protection strategy and its practical implementation.

4) Do-Not-Call Registry Provision

In essence, the protection model of PDPA 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”. In this regard, the DNC provisions were issued to avoid increasing dependence on personal smart devices and more aggressive digital marketing strategies adopted by many organizations. The DNC provisions are set out in Part IX of the PDPA. These deal with the establishment of Singapore’s national DNC and the obligations of organizations relating to the sending of particular marketing messages to Singapore telephone numbers. The DNC provisions comprise three separate registers kept and maintained by the PDPC under section 39 of the PDPA, which covers telephone calls, text messages, and faxes. The users and subscribers will be able to register their Singapore telephone number(s) on one or more DNC registers depending on their preferences in receiving marketing messages through telephone calls, text messages, or faxes. In this case, the organization has the following obligations regarding sending particular marketing messages to Singapore telephone numbers: (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 authorized the sending of the marketing message; and (3) not concealing or withholding the calling line identity of the sender of the marketing message.

Indonesia has been named the third-most spammed country in the world by Truecaller (a Swedish-based smartphone application company). According to the latest Truecaller Insights Report 2019, Indonesian users currently receive up to 27.9 spam calls per month for marketing purposes, with financial services (40%) and insurance brokers (23%) identified as the country’s top spammers. All these spam calls were sent to the Indonesian citizens without consent. Based on my research, Indonesia’s main data protection regulations are silent on the sending of unsolicited commercial or marketing communications. Implicitly,

174 Sirie (n 168).
175 ibid.
176 Klug (n 172).
178 Chik (n 147).
180 ibid.
the OJK has prohibited telemarketing telephone calls or texts by prohibiting businesses in the financial services sector from making any product or service offering or marketing to consumers and/or the public through private communication facilities without the prior consent of the consumer through its Regulation No. 1/2013. However, there are no other regulations on advertising and marketing as under Indonesian laws and regulations. It is subject to the general requirement for the obtainment of the consent of the data subject. Therefore, the Indonesian policymakers can learn and adopt the DNC provisions as implemented by Singapore in the future Indonesian data protection legal framework.

4.5 Interim Conclusion

This chapter aimed to analyze the GDPR of the EU and the PDPA of Singapore to highlight the key elements of these regulations that I believe Indonesian policymakers must pay attention to in drafting the new Indonesian data protection law. The key elements are (i) harmonization of the current Indonesian regulations, (ii) mandatory designation of DPA, (iii) mandatory designation of DPO, and (iv) DNC Registry Provision. These elements have been selected not only because of their immense impact in strengthening data protection in the EU and Singapore but also because Indonesian policymakers’ transposition into the upcoming law will effectively address the gaps in the current fragmented Indonesian data protection framework, as seen in Chapter 2. These aims have been addressed in Section 4.4, where I have listed out four important suggestions which I believe must be implemented in the new law in order for it to effectively redress the current problems of Indonesian data protection law.

---

182 Businesses in the financial services sector are defined as commercial banks, rural banks, securities companies, investment advisors, custodian banks, pension funds, insurance companies, reinsurance companies, multi-finance institutions, pawn companies, and guarantee companies that operate under conventional or sharia arrangements.
CHAPTER 5 - CONCLUSION

Indonesia has the potential to transform itself into a robust digital economy in the future. However, despite the widespread adoption of “disruptive” technologies, such as mobile internet, cloud computing, the Internet of Things and Big Data analytics, poor quality of services, uneven digitization across the country, and unregulated digital infrastructure are the main challenges which the country faces in unlocking its economic potential.\(^{183}\)

A key factor in creating this potential is the small yet growing base of digital consumers in the country, evidenced by the connectedness of the active online population. From the McKinsey survey quoted above, it becomes clear that social media usage and e-commerce usage are exceptionally high in Indonesia – with the most social media usage amongst any population in the world and 78% of all internet users making e-commerce transactions, most of which have been made with mobile phones.\(^{184}\) Furthermore, in the wake of the Covid-19 crisis, the national e-commerce policy (GR 80), which calls for the digitization of MSME’s across the nation, will play a crucial role in developing the infrastructure of the country.\(^{185}\) These strides towards digitization warrant a high standard of data protection for the citizens of the country.

Despite the progress mentioned earlier, Indonesia’s data protection regulation is vastly fragmented and plagued with various obstacles, which does not bode well for Indonesian citizens in the future. This thesis has aimed to address this very concern, hence at the beginning of Chapter 2, the description of the vast framework of data protection laws in Indonesia was addressed to highlight the fact that it is exceptionally fragmented across numerous sectors. The core elements of data protection are restricted to a few important regulations (EIT Law, GR 71/2019, and MoCI 20/2016), and the Ditjen Aptika carries out the enforcement of these regulations. Furthermore, the nature of the penalties imposed by this regulation and how Indonesian courts had handled data protection proceedings were also discussed.

In light of the drawbacks of existing Indonesian laws, Chapter 3 aimed to identify these drawbacks from regulatory, institutional, and cultural standpoints. While the drawbacks from both the fragmented regulations and their enforcement were explained, the cultural problems Indonesia faces in light of ensuring an adequate standard of data protection of its citizens is unique; the Indonesian citizens do not consider privacy and personal data security as an inherent part of their rights although they know that their data is being traded enormously. Thus, unlike the challenges faced by the EU and Singapore, which were briefly discussed in Chapter 4, Indonesia also has the added challenge of spreading awareness amongst its citizens by ensuring that relevant concepts associated with data protection and the right to privacy are needed to be disseminated effectively amongst the public.

Therefore, Chapter 3 concluded with suggestions that Indonesian regulators must consider in light of the unique problems faced by Indonesian regulators at present. However, the aim of Chapter 4 was also to highlight the elements of the European GDPR and the PDPA of Singapore – which the GDPR is renowned as a comprehensive data protection regime and the PDPA as a comprehensive tool for enabling and supporting the digital market – which I believe can further address the drawbacks mentioned in Chapter 3. Besides discussing the notable provisions of both regulations, I have also provided four suggestions that I believe Indonesian lawmakers must adopt from these laws while drafting the upcoming Indonesian law.

---


\(^{184}\) ibid.


43
By analyzing the above data protection frameworks (of the EU and Singapore), it can be concluded that the harmonization of data protection regulations in a successful data protection regime is an important element in ensuring a greater degree of security towards the protection of the data of citizens. Thus, harmonization of the current Indonesian sectoral regulations can be presumed to solve the overlap inadequacies in existing sectoral regulations.

The next essential suggestion is that Indonesia should have a designated DPA (by adopting the DPA concepts used in the GDPR and the PDPA) to carry out the supervision activity, currently being undertaken by the MoCI and Ditjen Aptika; as they are not specifically designated to tackle issues regarding data-protection-related matters. Further, a designated DPO is also one of the suggestions that might be effective to oversee the data protection responsibilities within the companies that collect and process the Indonesian citizens’ personal data. Besides, having extra help from the DPO to take care of the data compliance task will assist the supervisory/governmental authority in providing other data protection tasks such as providing guidance, enforcement actions, etc.

Further, it is also suggested to adopt the DNC provision from the PDPA in order to filter the spam messages such as direct marketing messages or free advertising that are being distributed through telephone calls, text messages, or faxes. Having the DNC provision in the future data protection legal framework will add more protection of the Indonesian citizens’ personal data and is expected to minimize the current problem in the Indonesian data protection regulations patchwork.

With the Indonesian government proposing to originally conclude the proposed personal data protection bill in November 2020\textsuperscript{186}, it is hoped that the government will make a stronger effort to take into account the concerns of citizens while drafting the bill, and I hope that the current problems plaguing the data protection law of Indonesia will ultimately be resolved to help the country realize its true potential as a powerful digital economy.

BIBLIOGRAPHY

Primary Sources

Regulations:

1. 1945 Constitution of the Republic of Indonesia
2. Brazil Lei Geral de Proteção de Dados
4. Data Protection Directive 95/46/EC
5. General Data Protection Regulation (Regulation (EU) 2016/679)
7. Government Regulation No. 82 of 2012 on the Implementation of Electronic System and Transactions
8. Law No. 1 of 1946 on Indonesian Criminal Code/Wetboek van Strafrecht/Kitab Undang-Hukum Pidana
9. Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking
10. 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
11. Law No. 14 of 2008 on Public Information Disclosure
12. Law No. 15 of 2003 on Stipulation of Government Regulation in lieu of Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism, became Law
13. Law No. 17 of 2011 on State Intelligence
14. Law No. 18 of 2003 on Advocate
15. Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission
16. Law No. 18 of 2014 on Mental Health
17. Law No. 21 of 2007 on Eradication of Human Trafficking/Undang-Undang Pemberantasan Tindak Pidana Perdagangan Orang
18. Law No. 21 of 2008 on Sharia Banking
19. Law No. 21 of 2011 on OJK
20. Law No. 23 of 1999 on Bank Indonesia
21. Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration/Administrasi Kependudukan
22. Law No. 29 of 2004 on Medical Practice
23. Law No. 30 of 2002 on Corruption Eradication Commission
24. Law No. 31 of 1999 on Corruption Eradication/Undang-Undang Tindak Pidana Korupsi
25. Law No. 35 of 2009 on Narcotics
26. Law No. 36 of 1999 on Telecommunication
27. Law No. 36 of 2009 on Health
28. Law No. 36 of 2014 on Health Workers
29. Law No. 39 of 1999 on Human Rights/Undang-Undang Hak Asasi Manusia
30. Law No. 43 of 2009 on Archival
31. Law No. 44 of 2009 on Hospital
32. Law No. 7 of 2014 on Trade
33. Law No. 8 of 1981 on Criminal Procedural Law/Kitab Undang-Undang Hukum Acara Pidana
34. Law No. 8 of 1997 on Company Documents
35. Law No. 8 of 1999 on Consumer Protection
36. Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime
37. Law No. 9 of 2013 on Prevention and Eradication of Terrorism Crime Funding
38. MoCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems
39. OJK Regulation No. 1/POJK.07/2013 of 2013 on Consumer Protection in the Financial Services Sector
40. Singapore Personal Data Protection Act 2012 (Regulation No. 26 of 2012)
41. South Africa Protection of Personal Information Act

Case Laws:
1. Bandung District Court v Buni Yani [2017] Bandung District Court (Bandung District Court).

Secondary Sources

Books:

Journals:
10. Denham E, ‘Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice’ 1
14. Eddyono S and Djafar W, ‘Menyeimbangkan Hak: Tantangan Perlindungan Privasi Dan Menjamin Akses Keterbukaan Informasi Dan Data Di Indonesia’
15. Gan T, ‘Data and Privacy Protection in ASEAN - What Does It Mean for Businesses in the Region?’
24. Personal Data Protection Commission - Singapore, ‘ADVISORY GUIDELINES ON KEY CONCEPTS IN THE PERSONAL DATA PROTECTION ACT’
27. PWC, ‘Indonesia’s Progress on Data Protection’ [2020] Digital Trust NewsFlash 2
33. Trepte S and others, ‘A Cross-Cultural Perspective on the Privacy Calculus’ (2017) 3 Social Media and Society

Websites and Articles

4. KOMINFO: https://kominfo.go.id/content/detail/11715/komisi-i-indonesia-perlu-uuperlindungan-data-pribadi/0/sorotan_media. Last accessed 26 December 2019
Official Documents

1. Otoritas Jasa Keuangan (Financial Services Authority), 'Otoritas Jasa Keuangan Dan BARESKRIM POLRI Sepakat Berantas Fintech Peer-To-Peer-Lending Ilegal Dan Investasi Ilegal' (Satgas Waspada Investasi 2019).
ANNEX 1

Following are the details of provisions of laws and sectoral regulations that address privacy and data protection provisions:

1) Law No. 1 of 1946 on Indonesian Criminal Code/Wetboek van Strafrecht/Kitab Undang-Undang Hukum Perdata (KUHP)

   Personal data protection in KUHP is stipulated in Chapter XXVIII concerning Crimes committed by officials, especially in Articles 430-433. Generally, the articles regulate civil servants’ or officials’ obligation to maintain confidentiality while performing activities involving personal data belonging to someone else.

   For example, Article 430(1) KUHP stipulates that an official is considered to be overstepping his competence when he causes to be produced to himself or seizes a letter, postcard, document or parcel, or telegraphic news entrusted to any public institution of transport. Of such actions, the civil servant or official is threatened by a maximum imprisonment period of two years and eight months. The same punishment shall be imposed upon any civil servant or official who in exercising his powers causes himself to be informed by an official of the telephonic services or by other persons charged with the services of a telephonic institution used for the general good, on the subject of a conversation which has taken place through the said institution.

   In Article 431 KUHP, it is also mentioned that the officials of the public transport institution are threatened by a maximum imprisonment period of two years if he deliberately intents and unlawfully opens a letter, sealed document, or parcel entrusted to such institution, examines it, or reveals the contents to another. While Article 432 KUHP regulates that any official of a public transport institution who deliberately delivers a letter, postcard, document or parcel entrusted to such institution to another than the rightful claimant, destroys, mislays, appropriates said letter, postcard, document, or parcel, or changes the contents or appropriates any article enclosed therein, shall be punished with a maximum imprisonment period of five years.

   Further, Article 433 KUHP mentions specifically that an imprisonment punishment threatens the public servant or official who has the authority to oversee telephone technology users’ activities if he leaks the contents of conversations to others or destroys and changes them unilaterally.

   Even though it is not explicitly mentioned in the articles, the KUHP clearly has some importance in terms of protecting personal data. This can be evidenced using criminal punishment for any violation related to personal data management, especially for civil servants or officials who have the duty and authority to access them.

2) Law No. 8 of 1981 on Criminal Procedural Law/Kitab Undang-Undang Hukum Acara Pidana (KUHAP)

   In accordance with Article 47 KUHAP, the police have the authority to access someone’s private letter sent through the post office, including information through telecommunications technology. This authority must go through the procedure of obtaining special permission from the Chief of the District Court. The obtainment of such permit indicates a form of pre-facto supervision or supervision before such interception is conducted. In addition, access is also

---

187 Article 430(1) of Law No. 1 of 1946 on Indonesian Criminal Code.
188 Article 430(2) of Law No. 1 of 1946 on Indonesian Criminal Code.
189 Article 431 of Law No. 1 of 1946 on Indonesian Criminal Code.
190 Article 432 of Law No. 1 of 1946 on Indonesian Criminal Code.
191 Article 433 of Law No. 1 of 1946 on Indonesian Criminal Code.
192 Djafar, Sumigar and Setianti (n 11).
limited to private letters that are suspected, with strong reasons, to relate to the criminal case being investigated.\textsuperscript{193}

Even though this provision in the KUHAP allows the violation of the right to privacy in some instances, the article also protects personal data for data subjects as reflected from the safeguards required to access personal data through special judicial permission and limited access only to specific data.\textsuperscript{194}

3) Law No. 8 of 1997 on Company Documents (Company Documents Law)

The Corporate Documents Law is intended to complete the provisions concerning the archive principle, which more regulates public aspects, within the scope of the company. Based on Article 1 Company Documents Law, the terminology of company documents is defined as data, records, or information made and/or received by companies to perform their activities, either written on paper or other media or recorded in any form that can be seen, read, or heard.\textsuperscript{195} Based on the type, Article 2 Company Documents Law expressly classifies the company documents consisting of financial documents and other documents.\textsuperscript{196, 197} The variety of the other documents may include the customer data and employee data, which are supposed to be classified as personal data.

In light of the above, this law allows a company to store other documents based on the retention schedule that has been determined by the head of the company,\textsuperscript{198} whereas the duration of such storage does not affect the function of the documents as evidence, with regard to the expiration terms of a claim.\textsuperscript{199, 200}

The company documents can also be transferred to the National Archives of Republic of Indonesia/Arsip Nasional Republik Indonesia (ANRI) based on the decision of the company’s leadership, as long as such document has a use-value for the national interest.\textsuperscript{201} In terms of document deletion, Indonesian Company Documents Law confirms that this can be conducted based on a predetermined retention schedule.\textsuperscript{202} Furthermore, the company is obliged to make an official report regarding the deletion of such documents.\textsuperscript{203}

Even though this law does not explicitly regulate personal data, the abovementioned articles show that the Company Documents Law protects personal data to some extent. This can be reflected in the existence of the document retention period and the deletion of such documents.

4) Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking (Banking Law)

Banking Law regulates a range of banking institutions’ activities, including bank secrecy, which is based on the principle of confidentiality, which requires banks to keep the confidentiality

\begin{footnotes}
\footnotetext{193}{Article 47 of Law No. 8 of 1981 on Criminal Procedural Law.}
\footnotetext{194}{Djafar, Sumigar and Setianti (n 11).}
\footnotetext{195}{Article 1 of Law No. 8 of 1997 on Company Documents.}
\footnotetext{196}{Reda Manthovani, \textit{Penyadapan vs. Privasi}, (Jakarta: Bhuana Ilmu Populer, 2013) p. 299 [Manthovani].}
\footnotetext{197}{Article 2 of Law No. 8 of 1997 on Company Documents.}
\footnotetext{198}{Article 11(3) and Article 11(4) of Law No. 8 of 1997 on Company Documents.}
\footnotetext{199}{Article 11(5) of Law No. 8 of 1997 on Company Documents.}
\footnotetext{200}{Djafar, Sumigar and Setianti (n 11).}
\footnotetext{201}{Article 18(1) of Law No. 8 of 1997 on Company Documents.}
\footnotetext{202}{Article 19(2) of Law No. 8 of 1997 on Company Documents.}
\footnotetext{203}{Djafar, Sumigar and Setianti (n 11).}
\end{footnotes}
related to data and information regarding customers, both their financial situation and personal information.  

In Article 1(28) Banking Law, bank secrets are interpreted as everything related to the information regarding depositing customers and their deposits. Thus, the principles of trust and confidentiality as the foundation of the financial institutions’ performance are also applied in the relationship between the customers and the bank. In savings or other bank products, the customer must provide personal data as it is deemed necessary for the bank. This relationship must be supported by bank’s the ability to maintain customer’s trust and protect the privacy of the customers who have provided the personal data. Article 40 states that the banks are obliged to keep the confidentiality of the information regarding depositing customers and their deposits, except in some instances in which it is allowed to be enclosed. The regulation implies that the customers’ privacy protection is related to their financial data (deposits or other bank products) and the customers’ personal data that is considered non-financial data. This obligation is strengthened by the presence of Article 47(2), which confirms the existence of imprisonment at least for 2 (two) years period and a fine of a minimum of IDR4,000,000,000 (four billion Indonesian Rupiah) and at a maximum of IDR8,000,000,000 (eight billion Indonesian Rupiah).

5) Law No. 8 of 1999 on Consumer Protection/Undang-Undang Perlindungan Konsumen (UUPK)

The current trading practices reflect that the consumers’ personal data is frequently obtained when they use a service or purchase an item or goods. For example, when conducting an online transaction, the consumer must provide their personal information to fulfill the transaction process. Later, the submitted personal information is misused for particular interests.

However, ironically, the protection guarantees towards the consumers’ data or information recognized in the Banking Law are not being followed by the UUPK. This instrument only regulates data protection or information on goods and services, as reflected in Article 9(1) UUPK, where it is prohibited to offer, produce, and advertise goods and/or services incorrectly. Even though the UUPK provides the criminal punishments for the violations of such provision, this criminal punishment has not accommodated the remedy for the victims or consumers whose personal data have been abused through direct sale and purchase of the consumers’ data.

6) Law No. 23 of 1999 on Bank Indonesia (Bl Law)

Same as the Banking Law and Law No. 21 of 2008 on Sharia Banking (Sharia Banking Law), Article 24 and 27 Bl Law strengthen the recognition of Bank Indonesia (BI)’s authority to conduct the oversight of banking activities in Indonesia, including matters pertaining to the disclosure of customers’ personal data by the bank to the matters related to the formation of an independent institution that specifically carries out the supervision activities. This law also allows BI to

---

205 Article 1(28) of Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking.
206 Article 40 of Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking.
207 Article 47(2) of Law No. 10 of 1998 on Amendment of Law No. 7 of 1992 on Banking.
208 Djafar, Sumigar and Setianti (n 11).
209 ibid.
210 Article 9(1) of Law No. 8 of 1999 on Consumer Protection.
211 Djafar, Sumigar and Setianti (n 11).
212 Article 24 of Law No. 23 of 1999 on Bank Indonesia.
213 Article 27 of Law No. 23 of 1999 on Bank Indonesia.
delegate the supervision authority to other parties to act on behalf of BI to carry out the examination to the inspected bank while maintaining the data confidentiality element obtained during the examination period.\textsuperscript{214}

7) Law No. 31 of 1999 on Corruption Eradication/Undang-Undang Tindak Pidana Korupsi (Tipikor Law)

Since the reformation era, the efforts to eradicate corruption in Indonesia have been strengthened. One of the efforts is from law reform. Several laws and regulations were established to strengthen law enforcement on corruption. The strengthening can be seen from the special authority granted to the Corruption Eradication Commission/Komisi Pemberantasan Korupsi (KPK). It is often for such special authority to intersect with the right to privacy of the parties who are alleged as the perpetrators of corruption. For example, the elucidation of Article 26 Tipikor Law stipulates that in the investigation, prosecution, and examination process of corruption cases, the investigator can carry out the wiretapping.

Besides wiretapping, the right to privacy restrictions are also reflected in Articles 28, 29, and 30 Tipikor Law. Article 28 stipulates the suspect’s obligation to provide information related to his family assets, including his wife, children, and his corporation.\textsuperscript{215} Further, Article 29 stipulates that the bank can be requested for the information of the suspect’s wealth data.\textsuperscript{216} In fact, paragraph 4 of such article stipulates that the law enforcement officers such as investigators, public prosecutors, or judges can request the bank to block the suspect’s savings account.\textsuperscript{217} Article 30 also provides authority for the investigator to open, inspect, and confiscate letters and items by post or other communication devices that belong to the suspect.\textsuperscript{218} All these authorities are exercised by the investigator based on sufficient evidence and only to those that are suspected of being related to the said corruption case.

With regard to personal data protection, the Tipikor Law does not discuss the further detailed mechanism relating to the privacy and data protection of the suspect and his family. However, in terms of confidentiality of the reporter’s identity, this law emphasizes that the witness and other people in the proceedings are prohibited from mentioning their personal data such as names, addresses, or things, which could open the possibility of revealing the true identity of the reporter.\textsuperscript{219} \textsuperscript{220}

8) Law No. 36 of 1999 on Telecommunication (Telecommunication Law)

Since 1980, Indonesia has actively opened the investment flows for the telecommunications industry. In terms of legal policy, in 1989, Indonesia began to develop regulations in the telecommunications sector in issuing Law No. 3 of 1989 on Telecommunications which later on in 1999, such law was replaced with the Telecommunication Law, which opens up the investment in telecommunication field for private entities (previously, the shares on telecommunication sector can only be owned by the state-owned enterprises).\textsuperscript{221}

\textsuperscript{214} Djafar, Sumigar and Setianti (n 11).
\textsuperscript{215} Article 28 of Law No. 31 of 1999 on Corruption Eradication.
\textsuperscript{216} Article 29 of Law No. 31 of 1999 on Corruption Eradication.
\textsuperscript{217} Article 29(4) of Law No. 31 of 1999 on Corruption Eradication.
\textsuperscript{218} Article 30 of Law No. 31 of 1999 on Corruption Eradication.
\textsuperscript{219} Article 31 of Law No. 31 of 1999 on Corruption Eradication.
\textsuperscript{220} Djafar, Sumigar and Setianti (n 11).
\textsuperscript{221} ibid.
The Telecommunications Law regulates the legal protection of the citizens’ freedom in communicating, including privacy and personal data protection. This can be reflected in Article 40 and Article 42 Telecommunications Law that explicitly prohibits all forms of wiretapping of information transmitted through the telecommunication networks and obliges the telecommunications service providers to maintain the confidentiality of information of the telecommunications service users. However, there is an exception to this provision, where the wiretapping activity is allowed as long as it is carried out for the interest of the criminal proceedings based on a written request of the Attorney General and/or the Chief of Police, and authorized investigators.  

In the event that wiretapping practice is carried out and exceed the allowable conditions, then the violators can be imprisoned to a minimum of two years or a maximum of 15 years and/or pay a maximum fine of IDR200,000,000 (two hundred million Indonesian Rupiahs).

9) Law No. 39 of 1999 on Human Rights/Undang-Undang Hak Asasi Manusia (HAM Law)

Privacy is a fundamental right that has to be guaranteed by law. Although the guarantee of human rights protection has been stipulated in the Indonesian Constitution as a constitutional basis, HAM Law provides more detail regarding the human rights itself.

There are several related articles in the context of privacy and data protection, namely Article 29(1), Article 31, and Article 32. In General, Article 29(1) HAM Law stipulates the recognition of each person’s personal protection, family, honor, dignity, and property rights. Meanwhile, Article 31 HAM Law stipulates that someone’s residence “should not be disturbed”. This article’s elucidation reflects that the context of such phrase refers to personal life (privacy) in his place of residence.

Another important thing in HAM Law is Article 32 that also regulates that the independence and secrecy in communications through electronic devices are guaranteed. However, this article can be exempted if there is an order from the judge or other authorized parties that have the authority to do so in accordance with the applicable legislation. From this article, it can be concluded that this provision provides a limitation of someone’s enjoyment of his right to privacy.

Furthermore, in the context of enforcement, HAM Law has mandated the National Commission of Human Rights/Komisi Nasional Hak Asasi Manusia (Komnas HAM) to carry out their function in conducting assessment, research, counseling, supervision, and mediation regarding human rights, including the issue of the right to privacy and personal data protection.

10) Law No. 30 of 2002 on Corruption Eradication Commission/Undang-Undang Komisi Pemberantasan Korupsi (KPK Law)

To eradicate corruption comprehensively, especially in carrying out the investigation and prosecution tasks, KPK Law provides several authorities to KPK to take actions that can intervene in someone’s right to privacy. This provision is stipulated in Article 12 KPK Law, specifically on

---

222 ibid.
223 Article 56 and Article 57 of Law No. 36 of 1999 on Telecommunication.
224 Article 29(1) of Law No. 39 of 1999 on Human Rights.
228 Article 76(1) and Article 89 of Law No. 39 of 1999 on Human Rights.
229 Djafar, Sumigar and Setianti (n 11).
letters (a), (c), and (f), specifies stipulates that the KPK has the authority to wiretap and record communication contents, request financial information of the suspects or defendants, and request the wealth and taxation data to the related banks or financial institutions.  

The KPK Law indirectly limits the investigators to access the personal data of the suspects and defendants. Such access can only be granted to the investigators if the data is related to the acts of corruption, such as assets and taxation. However, KPK Law does not provide further details regarding data management for the data that has been obtained by the KPK, primarily related to wiretapped data.  

Even according to Article 47 KPK Law, the KPK investigators are allowed to carry out the confiscation without the Chief of the District Court’s permission in the event that they already have sufficient initial evidence.

There is a lack of regulation on the wiretapping authority. An example can be reflected from the Tipikor Law. It is stipulated that the obtainment of evidence through wiretapping is possible if there is an allegation and report that there is a corruption act or there will be a corruption act.  


As one form of national and international commitment to eradicating terrorism, Indonesia established the Anti-Terrorism Law, which was previously a Government Regulation No. 1 of 2002. This regulation regulates some provisions regarding law enforcement with special authorities to eradicate terrorism. Such authorities are wiretapping and accessing the personal data of citizens suspected of being involved in terrorism crime.

Article 29 Anti Terrorism Law authorizes the investigators, public prosecutors, or judges to order banks and financial service institutions to block the assets of every person that is known or suspected as a result of terrorism and/or any terrorism-related criminal activity. In implementing such authority, paragraph (2) requires the investigator to make a warrant that contains clear information of the identity of the investigators, public prosecutors or judges, identity of the party that is reported by the bank, reasons for account blocking, suspected or indicated crime, as well as the location of the wealth or assets.

Article 30 Anti-Terrorism Law allows the investigator to investigate the wealth of the suspected party or known for committing criminal acts of terrorism. Paragraph 2 of the same article emphasizes that this article can exempt the provision of the law that regulates bank confidentiality and financial transaction confidentiality. However, a warrant that contains precise information on the identity of the investigator, the identity of the person who committed

230 Article 12(a), Article 12(c), and Article 12(f) of Law No. 30 of 2002 on Corruption Eradication Commission.
231 Djafar, Sumigar and Setianti (n 11).
232 Article 47 of Law No. 30 of 2002 on Corruption Eradication Commission.
233 Elucidation of Article 28(1) of Law No. 31 of 1999 on Corruption Eradication.
234 Djafar, Sumigar and Setianti (n 11).
236 Article 29(2) of Government Regulation in lieu of Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism.
238 Article 30(2) of Government Regulation in lieu of Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism.
the crime, the type of crime, and the location of the wealth or assets is obliged to be obtained before such request can be made.

Article 31 Anti-Terrorism Law also stipulates that if there is sufficient preliminary evidence, the investigator has the right to access personal data of the suspect, such as letters, and wiretap the telephone conversations or other communication devices. Wiretapping action can only be carried out by the Chairman of the District Court’s order within one year. Further, even though it does not clearly regulate the recognition of the right to privacy, Article 32 regulates the obligation to keep the confidentiality of personal data regarding witnesses and reporters. In paragraph (2), it is stated that witnesses and others who are related are prohibited from mentioning the reporter’s identity in the proceedings. This is intended to provide security and protection for the witnesses and reporters.

12) Law No. 18 of 2003 on Advocate (Advocate Law)

One of the obligations of an advocate in carrying out his profession is to protect his client’s confidentiality. This is emphasized in the Advocate Law that stipulates that an advocate must keep everything known or obtained from his client because of his professional relationship unless otherwise specified by law. Such confidentiality includes protecting the files and documents against confiscation or inspection and protection against wiretapping towards the advocate’s electronic communication. From this provision, it is reflected that the secrets of advocates and their clients can only be opened if the law says so.

However, there is a new problem since the issuance of Government Regulation No. 43 of 2015 on the Reporting Party in the Prevention and Eradication of Money Laundering. Article 3 of this regulation obliges the lawyers to report to the Financial Report and Analysis Center/Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) if there is a suspicion of money laundering from his service user. This provision is contradicted with the provision as stipulated in the Advocate Law as elaborated above.

13) Law No. 29 of 2004 on Medical Practice (Medical Practice Law)

In general, the Medical Practice Law regulates standards of doctor practice, specifically, the service standards for patients, the administrative procedures that must be taken to carry out the practice, the rights and obligations of a doctor, as well as the supervision and sanctions for the practicing doctors. In principle, every medical performance recognizes the privacy of patients regarding their medical records. Article 47(2) Medical Practice Law stipulated that a doctor must maintain his patient’s medical record’s confidentiality as one of the patient’s rights that must be protected. Such matter is even more emphasized in Article 48(1), where the doctor is obliged to

---

241 Article 32(2) of Government Regulation in lieu of Law No. 1 of 2002 on Eradication of Criminal Acts of Terrorism.
242 Djafar, Sumigar and Setianti (n 11).
243 Article 19 of Law No. 18 of 2003 on Advocate.
244 Djafar, Sumigar and Setianti (n 11).
245 ibid.
246 Article 47(2) of Law No. 29 of 2004 on Medical Practice.
to keep the confidentiality of the patient’s medical record forever even after the patient has passed away.\textsuperscript{247}

However, there is an exemption in certain conditions where the patient’s medical record’s confidentiality can be disclosed as stipulated in Article 48(2) Medical Practice Law. Certain conditions are limited only for the benefit of the patient’s health, in the context of law enforcement, request by the relevant patient, or based on the legislation.\textsuperscript{248}

Under Article 64 Medical Practice Law, a mechanism that guarantees the personal data protection is carried out by the Indonesian Medical Disciplinary Board/\textit{Majelis Kehormatan Disiplin Kedokteran Indonesia}. This article elaborates on the complaint’s procedure and examining and deciding the doctors’ violation cases. As mentioned previously, the leakage of the patient’s medical record or data is also considered a violation. The complaint mechanism is regulated in Article 66 until Article 70 Medical Practice Law. The doctor will be threatened by a maximum of one year of imprisonment or a fine of maximum IDR50,000,000 (fifty million Indonesian Rupiah) if he does not carry out the obligation to maintain patient health secrets.

Further, the technical regulations regarding the confidentiality of medical records are regulated in the Minister of Health Regulation No. 36 of 2012 on Medical Confidentiality. This regulation regulates further regarding the scope of medical confidentiality and its supervision. According to this regulation, medical confidentiality can be exempted for the benefit of the patient’s health, in the context of law enforcement, requested by the relevant patient, or based on the legislation.\textsuperscript{249}

14) \textit{Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration/\textit{Administrasi Kependudukan} (Adminduk Law)}

The Adminduk Law regulates the population administration activities as part of structuring and controlling activities in the issuance of documents and data of the population, including the citizens’ personal data\textsuperscript{250} through the Population Administration Information System/\textit{Sistem Informasi Administrasi Kependudukan} (SIAK). Article 1(22) Adminduk Law recognizes personal data as data that has to be kept, cared for, and protected its truth and confidentiality.\textsuperscript{251} According to Article 85 Adminduk Law, the state must preserve and protect the population’s personal data.\textsuperscript{252} Article 79 also stipulates that the state has an obligation to provide protection and appoint the minister as the person-in-charge of the access right of the population’s personal data.\textsuperscript{253}

The existence of the abovementioned articles causes the access right of the operator and implementing institutions that collect the personal data of the population to keep the information and the confidentiality of such data. However, this regulation has not fully accommodated the protection of the personal data of the population.\textsuperscript{254}

In terms of the mechanism for the violations recovery, the Adminduk Law recognizes the right of the population to obtain compensation and recovery due to the misuse and abuse of

\textsuperscript{247} Article 48(1) and Article 51(c) of Law No. 29 of 2004 on Medical Practice.
\textsuperscript{248} Article 48(2) of Law No. 29 of 2004 on Medical Practice.
\textsuperscript{249} Djafar, Sumigar and Setianti (n 11).
\textsuperscript{250} Article 84(1) Adminduk Law emphasizes some data that fell into the category of citizens’ personal data, namely: (a) KK; (b) NIK; (c) date, month or year of birth; (d) information concerning physical and/or mental disability; (e) NIK of the biological mother; (f) NIK of the father; and (g) some records of the important events.
\textsuperscript{251} Article 1(22) of Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration.
\textsuperscript{252} Article 85 of Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration.
\textsuperscript{253} Article 79 of Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration.
\textsuperscript{254} Djafar, Sumigar and Setianti (n 11).
personal data by the implementing institutions.\textsuperscript{255} Further, Article 95 emphasizes that there is a punishment of \textit{It} for a maximum of two years and a fine of IDR25,000,000 (twenty-five million Indonesian Rupiah) against the parties who unlawfully access the population database.\textsuperscript{256}

15) Law No. 21 of 2007 on Eradication of Human Trafficking/\textit{Undang-Undang Pemberantasan Tindak Pidana Perdagangan Orang} (TPPO Law)

To eradicate the crime of human trafficking in Indonesia, the TPPO Law provides several authorities to intrude on the citizens’ right to privacy. Such authorities are the authority to conduct wiretapping and access the personal data of the human trafficking suspects. With regard to the investigation, the elucidation of Article 29 TPPO Law stipulates that the scope of “data” includes bank accounts, financial records, travel records, communications, and other documents.\textsuperscript{257} This means that the investigator has the authority to access the personal data of such human trafficking suspects. Even in Article 32 TPPO Law, it is stipulated that the investigators, public prosecutors, or judges are authorized to order the financial services providers to block the assets of the person suspected or convicted of committing a human trafficking crime.\textsuperscript{258}

With regard to the wiretapping, Article 31 TPPO Law stipulates that the investigators can carry out the wiretapping through the telephone or other communication devices as long as the investigators have preliminary evidence.\textsuperscript{259} Besides, Article 31(2) mentioned that prior written permission from the Chief of the District Court is required before the wiretapping is carried out.\textsuperscript{260}

In addition to the authority to wiretap and intrude on personal data, Article 33 TPPO Law emphasizes personal data protection for the witnesses and reporters. The reporters are entitled to request the investigator to maintain the confidentiality of their identities, such as name and address.\textsuperscript{261} Therefore, the investigator is obliged to keep the secrecy of their identity in the investigation, prosecution, and examination process in the court proceedings.\textsuperscript{262}

16) EIT Law

EIT Law mentioned implicitly regarding the protection of data or electronic information, both publicly and privately. The regulation also regulates the protection for unauthorized access, the protection by the electronic system providers, and the protection from illegal intervention access. All these protections can be reflected in Article 26 EIT Law, where it requires that the processing of any personal data in the electronic system must be based on the relevant data subject’s consent.\textsuperscript{263} The elucidation of this article stipulates that in the Information Technology, the protection of personal data is one part of the right to privacy, where it includes (i) the right to enjoy a personal life and be free from all kinds of disturbance; (ii) the right to be able to communicate with others (without spying); and (iii) the right to supervise the access regarding one’s personal life information and data.\textsuperscript{264}

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{255} Article 2(f) of Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration.
\item \textsuperscript{256} Article 95 of Law No. 24 of 2003 on Amendment of Law No. 23 of 2006 on Population Administration.
\item \textsuperscript{257} Article 29 of Law No. 21 of 2007 on Eradication of Human Trafficking.
\item \textsuperscript{258} Article 32 of Law No. 21 of 2007 on Eradication of Human Trafficking.
\item \textsuperscript{259} Article 31 of Law No. 21 of 2007 on Eradication of Human Trafficking.
\item \textsuperscript{260} Article 31(2) of Law No. 21 of 2007 on Eradication of Human Trafficking.
\item \textsuperscript{261} Article 33 of Law No. 21 of 2007 on Eradication of Human Trafficking.
\item \textsuperscript{262} Djafar, Sumigar and Setianti (n 11).
\item \textsuperscript{263} Article 26 of Law No. 11 of 2008 on Electronic Information and Transactions.
\item \textsuperscript{264} Elucidation of Article 26 of Law No. 11 of 2008 on Electronic Information and Transactions.
\end{itemize}
\end{footnotesize}
In addition, Article 43(2) stipulates the essence of personal data protection for the citizens, even in criminal proceedings. It is specified that any investigation related to Information Technology and Electronic Transactions must be carried out by upholding the protection of privacy, confidentiality, and data integrity in accordance with the applicable legislation. Furthermore, as regulated in KUHAP, the EIT Law emphasized that any search and/or confiscation of the electronic system related to the alleged crime must be carried out with the Chairman of the District Court’s permission.

With regard to the protection, EIT Law has provided the way to file a lawsuit on the loss caused by the abuse of personal data. Article 38 EIT Law stipulates that each party that suffers a loss or disadvantage because of the information technology and electronic system’s implementation can file a lawsuit. As for the wiretapping activity, as stipulated in Article 31 EIT Law, Article 47 EIT Law stipulates a punishment of imprisonment for a maximum of ten years and a fine of IDR800,000,000 (eight hundred million Indonesian Rupiah).

As the derivative regulation of EIT Law, the government issued GR 82/2012 as amended by the GR 71/2019, clearly stipulated regarding personal data protection. According to the said regulation, personal data is defined as any data on a person that is identified and/or may be identified individually or combined with other information both directly and indirectly through an electronic system and non-electronic system. One of the most protected data is the data that is related to electronic information. Article 1(8) GR 71/2019, electronic information is defined as one or a group of electronic data, including but not limited to text, voice, picture, map, design, photo, electronic data interchange, electronic mail, telegram, telex, telecopy or similar, letter, sign, number, access code, symbol, or perforation which has been processed which has meaning or may be understood by people who can understand it. The electronic information can be found in an electronic system or in the form of an electronic document. Article 4(b) GR 71/2019 also stipulates that the electronic system provider must maintain the confidentiality, integrity, and availability of the managed personal data.

Article 100 GR 71/2019 provides administrative sanctions for the electronic system provider and/or its agent who violates the provisions as stipulated above. The administrative sanctions as referred to in the previous sentence are as follows: (a) written reprimand; (b) administrative fine; (c) temporary suspension; (d) access termination; and/or (e) removal from the list of electronic system provider, electronic agent, and electronic certification provider.

17) Law No. 14 of 2008 on Public Information Disclosure (PID Law)

In making the right governance environment, the Indonesian government issued the law on public information disclosure. Based on Article 1(1) PID Law, information is defined as details, statement, ideas, and signs that contain values, meanings, and messages, both data, facts, and

---

265 Article 43(2) of Law No. 11 of 2008 on Electronic Information and Transactions.
266 Article 38 of Law No. 11 of 2008 on Electronic Information and Transactions.
267 Article 47 of Law No. 11 of 2008 on Electronic Information and Transactions.
270 Article 4(b) of Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions.
271 Article 100 of Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions.
272 Article 100(2) of Government Regulation No. 71 of 2019 on the Organization of Electronic Systems and Transactions.
explanations that can be seen, heard, read, presented in various packaging and formats following the electronic and non-electronic information technology and communication developments. While Public information is defined as the information that is generated, stored, managed, sent, and/or received by the public agency that is related to the organizer and organization of the state and/or organizer and organization of other public agency following this law and other information related with the public interests.

Even though the existence of this law helps to access data and information collected by the public agencies, there are exceptions for the personal-data-related information. In Article 6(3)(c) of PID Law, public agencies cannot disclose any personal rights information. Similar things also written in Article 17(g) and (h) which states that authentic deed that has a personal nature and one’s last will and information relating to personal secrets are considered excluded information. The information that can reveal personal secrets is the information related to history and family member condition, physical and psychological health treatment, financial condition, a person’s income, bank account, and formal and informal education history.

The existence of the abovementioned provisions reflects an obligation to protect the information relating to personal rights. In other words, PID Law provides the authority to exercise self-control in every public agency in the context of personal data protection to be not publicly disclosed.

18) Sharia Banking Law

Materially, the Sharia Banking Law has similar content with the Banking Law, including matters related to personal data protection. Article 41 of Sharia Banking Law regulates the bank’s mandate to maintain its customer data confidentiality, except for the tax investigation as stipulated in Article 42 to Article 49.

In such exception, Article 42(1) regulates the mechanism that must be implemented by law enforcement authorities, such as mentioning the name of the tax official, the name of the taxpayer as well as the details of the relevant case. Article 50 Sharia Banking Law has provided BI with authority to supervise every sharia banks’ activities, including those related to the enforcement of the principle of bank secrecy or confidentiality. However, please note that after the establishment of the OJK, such BI’s authority has been automatically transferred to the OJK.

Further, there are two types of sanctions that will be used in protecting the customers’ privacy, administratively, and criminally. Article 60 Sharia Banking Law stipulates that everyone who asks the bank to provide information without going through the applicable procedures is threatened by a minimum imprisonment of two years and a maximum of four years as well as a fine within IDR10,000,000,000 (ten billion Indonesian) to IDR200,000,000,000 (two hundred billion Indonesian Rupiah). In the banks’ internal arrangements, the bank officials and employees that do not fulfill the obligations to protect the customers’ personal data, threatened

273 Article 1(1) of Law No. 14 of 2008 on Public Information Disclosure.
274 Article 1(2) of Law No. 14 of 2008 on Public Information Disclosure.
275 Article 6(3)(c) of Law No. 14 of 2008 on Public Information Disclosure.
276 Article 17(g) and Article 17(h) of Law No. 14 of 2008 on Public Information Disclosure.
277 Djafar, Sumigar and Setianti (n 11).
278 Article 41 of Law No. 21 of 2008 on Sharia Banking.
279 Article 42(1) of Law No. 21 of 2008 on Sharia Banking.
280 Article 50 of Law No. 21 of 2008 on Sharia Banking.
281 Djafar, Sumigar and Setianti (n 11).
282 Article 57 of Law No. 21 of 2008 on Sharia Banking.
283 Article 60 of Law No. 21 of 2008 on Sharia Banking.
by a minimum imprisonment of two years and a fine of approximately IDR15,000,000,000 (fifteen billion Indonesian Rupiah).\textsuperscript{284}

19) Law No. 35 of 2009 on Narcotics (Narcotics Law)

This law provides authority to the National Anti-Narcotics Agency/\textit{Badan Narkotika Nasional} (BNN) to carry out the intervention of citizens’ right to privacy to eradicate narcotics crime. Such authority is related to the wiretapping and access to wealth and taxation data related to the misuse, illicit trafficking, and narcotics precursors committed by the suspects as stipulated in Article 75 (i) Narcotics Law.\textsuperscript{285} In practice, the mechanism of wiretapping for narcotics misuse is regulated in Article 77 Narcotics Law, where it stipulates that the wiretapping can be carried out after the investigators received sufficient preliminary evidence with a period of three months after the investigators obtain the wiretapping permission. Such wiretapping permission is obtained from the Chairman of the District Court.\textsuperscript{286}

However, Article 78 Narcotics Law allows investigators to carry out wiretapping without written permission from the Chairman of the District Court as long as the investigators request the written permission afterward within one day. In addition to wiretapping, the Narcotics Law also allows the investigators to access personal data related to the suspects’ wealth and taxation data.\textsuperscript{287}

20) Law No. 36 of 2009 on Health (Health Law)

In accordance with Article 52(2) Health Law, in conducting their duty, the health workers are obliged to comply with professional standards and respect patients’ rights, including the information of their medical records.\textsuperscript{288} Further, Article 57 Health Law stipulates that everyone has the right to privacy towards the medical records that have been disclosed to the health service providers. However, this right can be excluded if related to law enforcement and other interests as stipulated in Article 57(2).\textsuperscript{289}

The mechanism for protecting patient medical records can be interpreted as an obligation to organize health services as regulated in Article 54 Health Law. Such article mentioned that health services should be carried out safely, equally, and non-discriminatory. This article even emphasizes the Central Government’s tasks and Local Government for the health services, which can be interpreted, including the authority to maintain the privacy and confidentiality of patients’ medical records.\textsuperscript{290}

However, Health Law does not fully regulate the data subjects’ recovery mechanisms (in this case are the patients) for violations of their personal data. This law does not contain sanctions or penalties, both administratively and criminally, for the violators of such obligations.\textsuperscript{291}

21) Law No. 43 of 2009 on Archival (Archival Law)

\textsuperscript{284}Djafar, Sumigar and Setianti (n 11).
\textsuperscript{285}Article 75(i) of Law No. 35 of 2009 on Narcotics.
\textsuperscript{286}Article 77 of Law No. 35 of 2009 on Narcotics.
\textsuperscript{287}Article 78 of Law No. 35 of 2009 on Narcotics.
\textsuperscript{288}Article 8 and Article 52(2) of Law No. 36 of 2009 on Health.
\textsuperscript{289}Article 57 of Law No. 36 of 2009 on Health.
\textsuperscript{290}Article 54 of Law No. 36 of 2009 on Health.
\textsuperscript{291}Djafar (n 2).
In the process of state administrative activities, there is an organization of archival system by the government. This archival system often includes personal data or information of a person, for example, population data, teaching staff and students in the university, etc. The archival system is regulated in the Archival Law, which governs the state administrative organization’s public archival aspect. Article 3(f) Archival Law stipulates that one of archival purposes is to guarantee safety and security as proof of liability in the social, national, and state life. Meanwhile, as the guarantee towards such data security, the Archival Law has included the threat of administrative and criminal sanctions towards anyone who violates the usage of state archives based on provisions that have been provided in this law. The existence of the abovementioned provisions in the Archival Law reflects an obligation to protect the information relating to personal data.

22) Law No. 44 of 2009 on Hospital (Hospital Law)

Similar to Health Law, the protection of patient data against the implementation of medical recording activities carried out by a hospital is recognized in Article 29(1)(h), (l), and (m) Hospital Law. The acknowledgment of privacy is part of the patient’s rights as stated in Article 32(i). This is reiterated in Article 38(1) which requires hospitals to keep medical secrets and Article 44 which stipulates that the hospital can disclose any medical information to the public if the same information has been disclosed publicly by the patient or his family. The protection of the patients’ right to privacy can be reflected from Article 38(2) Hospital Law, where for the sake of law enforcement, the patient’s health data and medical record can be disclosed to related parties.

Concerning the mechanism procedure, Article 54 and 55 Hospital Law stipulates the Central Government and Local Government’s duties in conducting guidance and supervision of hospital by involving professional organizations and hospital associations. One of their duties also concerns the obligation to protect the confidentiality of patient health data which is the responsibility of the professions of health workers, including hospitals.

23) Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime (Money Laundering Law)

Based on the Money Laundering Law provisions, PPATK has the authority to carry out the action to intrude on citizens’ right to privacy, to prevent and eradicate money laundering crime. This law confirms that in carrying out their duties, PPATK has the authority to request and obtain data from government agencies and/or private institutions that have the authority to manage data, including from government agencies or private institutions that receive reports from certain professions. Further, Article 41(2) Money Laundering Law stipulates that the data or information accessible to PPATK is data relating to financial transactions resulting from criminal activities. PPATK’s authority, as stipulated above, is excluded from the obligation to maintain confidentiality.

---

292 Article 5(1) of Law No. 43 of 2009 on Archival.
293 Article 78 – Article 88 of Law No. 43 of 2009 on Archival.
294 Article 32(i) of Law No. 44 of 2009 on Hospital.
295 Article 38(1) and Article 44 of Law No. 44 of 2009 on Hospital.
296 Article 38(2) of Law No. 44 of 2009 on Hospital.
297 Article 44 and Article 45 of Law No. 44 of 2009 on Hospital.
298 Article 40 and Article 41(1) of Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.
299 Article 41(2) of Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.
Similar things are also stipulated in Article 45, where any Indonesian laws and regulations do not affect PPATK’s authority in maintaining confidentiality, as mentioned above. Further, Article 72(2) stipulates that in requesting information related to the money laundering case, the laws regulating the bank’s secrecy and other financial transactions do not apply to the investigators, prosecutors, and judges in charge.

In carrying out this task, PPATK employees and those who have the authority to obtain the documents and/or information must maintain its confidentiality, except for the fulfillment of the obligations under this law. Article 54(2) also mentioned that one of the oaths sworn by the Chairman and Vice-Chairman of PPATK is that they have to keep the confidentiality of any documents and/or information as mandated by the Indonesian legislation, including the obligation to maintain privacy in order to protect the reporters and witnesses.

24) Law No. 17 of 2011 on State Intelligence (Intelligence Law)

In carrying out state intelligence, the State Intelligence Agency/Badan Intelijen Negara (BIN) is given the authority to conduct wiretapping, check the flow of funds and information extraction from the suspicious activities in Indonesia. To obtain any information related to the state intelligence, BIN can request the law enforcers and related institutions for such information. The provision of this authority has some potential for the intrusion of someone’s personal data.

With regard to the above, Article 15(1) Intelligence Law gives space for the party who is abused because of the implementation of intelligence action to apply for rehabilitation, compensation, and restitution. Although it is not explained in detail what is meant by “abused because of the implementation of intelligence action”, but this can be interpreted as an intrusion of privacy because of the intelligence action. Further, another protection that is provided by this law is stipulated in Article 47, where any BIN personnel who conduct the wiretapping that is not related to the functions of investigation, security, and raising as specified in Article 32, shall be punished with the maximum imprisonment of five years and/or a maximum fine of IDR500,000,000 (five hundred million Indonesian Rupiah).

25) Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission (JC Law)

The existence of the Judicial Commission (JC) has the aim to build a fair and independent law enforcement environment. Therefore, the JC Law provides some authorities to JC, including restricting someone’s right to privacy. Article 20(3) stipulates that JC can request the law enforcers to conduct wiretapping and record the judge’s conversation if there is an alleged violation of the judicial code of ethics. In addition, to do supervision, JC can request information or data from the Judiciary/Badan Peradilan and/or judge through the Supreme Court as regulated in Article 22 JC Law. The data referred to in the previous sentence relates to the judicial process and ethical violation allegation.

26) Law No. 21 of 2011 on OJK (OJK Law)

300 Article 45 of Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.
301 Article 72 of Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.
302 Article 11(1) of Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.
303 Article 83 of Law No. 8 of 2010 on Prevention and Eradication of Money Laundering Crime.
304 Article 31 of Law No. 17 of 2011 on State Intelligence.
305 Article 20(3) of Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission.
306 Article 22 of Law No. 18 of 2011 on Amendment of Law No. 22 of 2004 on Judicial Commission.
During its development, the monitoring and supervision mechanism of the bank customers' personal data in the context of bank secrecy, which was previously the authority of BI, as stipulated in Banking Law, Sharia Banking Law, and BI Law, since the establishment of OJK Law, has been transferred to the OJK.\textsuperscript{307}

This provision is more emphasized through the issuance of OJK Regulation No. 1/POJK.07/2013 of 2013 on Consumer Protection in the Financial Services Sector (POJK Consumer Protection), which stipulates that there are basic principles of consumer protection that have to be maintained by the OJK, specifically consumer confidentiality and security data or information principles.\textsuperscript{308} The OJK even provides a detailed list of consumer data and/or personal information, which confidentiality must be maintained through the OJK Circular Letter No. 14/SEOJK.07/2014 on Confidentiality and Security of Consumer's Data and/or Personal Information, such as name, address, telephone number, date of birth and/or age, name of biological mother (specifically for individual customers), as well as the composition of the board of directors and board of commissioners, including identity document such as identity card, passport and/or stay permit, and/or composition of shareholders (specifically for corporate customers).

The existence of the abovementioned provisions reflects that there is an obligation to protect the information relating to personal data, in this context, is the bank customers' personal data.

27) Law No. 9 of 2013 on Prevention and Eradication of Terrorism Crime Funding (Terrorism Funding Law)

Supervision of the funding is considered one of the significant prevention efforts in eradicating terrorism crime because terrorism funding is one of the main factors in every act of terrorism. Therefore, the efforts to tackle terrorism must be conducted by the prevention and eradication of terrorism funding. In this context, the Terrorism Funding Law provides some authority to the government and law enforcement institutions to conduct observations and access the citizens' personal data who are indicated to be committing terrorism crime. The granting of authority has the potential to open loopholes and space for violation of the citizens’ right to privacy, especially related to personal data, especially banking-related data.\textsuperscript{309}

As additional security to maintain the confidentiality of these data, the provisions in the Terrorism Funding Law stipulate that PPATK officials or employees, investigators, prosecutors, judges, or any person who obtained or information relating to suspicious financial transactions, especially related to the terrorism funding, has an obligation to keep the confidentiality.\textsuperscript{310} This law also stipulates that if the relevant person leaks or discloses the confidential documents related to such funding, the relevant person will be threatened by a maximum imprisonment of four years.\textsuperscript{311} Further, the existence of this article reflects that there is personal data protection related to financial transactions that are suspected of being involved in terrorism funding.\textsuperscript{312}

\textsuperscript{307} Article 5, Article 6(a), and Article 7 of Law No. 21 of 2011 on Financial Services Authority.

\textsuperscript{308} Article 2(d) of OJK Regulation No. 1/POJK.07/2013 of 2013 on Consumer Protection in the Financial Services Sector.

\textsuperscript{309} Djafar, Sumigar and Setianti (n 11).

\textsuperscript{310} Article 9(1) of Law No. 9 of 2013 on Prevention and Eradication of Terrorism Crime Funding.

\textsuperscript{311} Article 9(2) of Law No. 9 of 2013 on Prevention and Eradication of Terrorism Crime Funding.

\textsuperscript{312} Djafar, Sumigar and Setianti (n 11).
28) Law No. 7 of 2014 on Trade (Trade Law)

The provisions of Trade Law do not specifically regulate the protection of consumers’ personal data. However, this law states that the trade using an electronic system or e-commerce, every trader has to refer to any applicable provision as stipulated in the EIT Law.\(^{313}\) It means that the EIT Law provisions regarding the protection of customers’ personal data are also fully binding for each trading that utilizes the electronic system.

As for the protection mechanism, Article 65(5) stipulates that any dispute relating to trade with the electronic system are settled through the district court and other dispute resolution mechanisms. This law also regulates administrative sanctions for business actors who do not fulfill the obligation to provide the data or information completely and correctly.\(^{314}\) There is no further explanation of the personal data protection provisions in this law.

29) Law No. 18 of 2014 on Mental Health (Mental Health Law)

One type of data regulated in the Mental Health Law is mental health data. Mental Health Law stipulates that people that are considered as Person with Psychiatric Problem/Orang Dengan Masalah Kejiwaan (ODMK) and Person with Mental Disorders/Orang Dengan Gangguan Jiwa (ODGJ) are entitled to obtain comprehensive and complete information regarding their mental health record that will be received from the practitioner that has competence in the mental health field.\(^{315}\) According to the abovementioned, it can be seen that medical practitioners have the authority to access personal data, specifically regarding mental health.

However, this law does not clearly regulate the mechanism of protection for collecting and processing that data. Article 75 Mental Health Law only mentions that the Central Government and Regional Government have duties and responsibilities to maintain any best effort related to the organization of mental health practice. The protection of personal data related to a person’s mental health is not included in such duties and responsibilities.\(^{316}\) Further, Mental Health Law allows mental health data to be disclosed for investigation and law enforcement interests.\(^{317}\)

30) Law No. 36 of 2014 on Health Workers (Health Workers Law)

In carrying out their work, the health workers will always intersect with patients’ health data, and medical records as one of the personal data types, the protection towards such health data and medical records should be guaranteed. The Health Workers law only regulates that health workers must fulfill their obligation to maintain the confidentiality of the patients’ health data and medical records.\(^{318}\)

However, Article 73(2) stipulates that the patient’s health data and medical records can be disclosed to the public for certain interests, such as law enforcement’s interests and requests by the patients. This law expressly regulates the data protection mechanism in the form of sanctions if a violation occurs. The person who violates the abovementioned provisions will be threatened by an administrative sanction in the form of oral reprimand, written reprimand, administrative fine, and/or revocation of the license by the government.\(^{319}\)

---

\(^{313}\) Article 65(3) of Law No. 7 of 2014 on Trade.
\(^{314}\) Article 65(6) of Law No. 7 of 2014 on Trade.
\(^{315}\) Article 68(d) and Article 70(1)(e) of Law No. 18 of 2014 on Mental Health.
\(^{316}\) Article 4 of Law No. 18 of 2014 on Mental Health.
\(^{317}\) Article 71 and Article 72 of Law No. 18 of 2014 on Mental Health.
\(^{318}\) Article 58(1) of Law No. 36 of 2014 on Health Workers.
\(^{319}\) Article 82 of Law No. 36 of 2014 on Health Workers.