PERSONAL DATA PROTECTION IN INDONESIA: THE LONG ROAD TO EFFECTIVE IMPLEMENTATION

RESEARCH NOTE

OPEN DATA LABS JAKARTA

WORLD WIDE WEB FOUNDATION

This research was written by Dinita Andriani Putri, Project Manager at the World Wide Web Foundation's Open Data Lab Jakarta.

Suggested Citation: Putri, Dinita A. (2019). *Personal Data Protection in Indonesia: The Long Road to Effective Implementation. Jakarta: World Wide Web Foundation.*

Acknowledgements: The author would like to acknowledge the key informants who participated in interviews to support this research. Teddy Woodhouse, Carlos Iglesias, Dhanaraj Thakur, and Glenn Maail from the Web Foundation for their insightful comments, and Sabine Matsheka and Kara Nash for the edits.

Executive Summary

This study explores the challenges in the implementation of the existing regulations on personal data protection and identifies strategies for the future Personal Data Protection Law in Indonesia. A desk study and expert interviews were used to gain in-depth information about the subject. The study was conducted to understand the legal framework of personal data protection in Indonesia and the challenges in the implementation of the existing legal frameworks.

Data protection regulation has become one of the most prominent regulations in today's data-based world. Implementing a data protection regulation has become delicate work, even for those that already had a comprehensive regulation, such as the EU. The scattered data protection-related regulation in Indonesia indeed is facing different implementation challenges.

This study observed three main challenges in the implementation of the regulation on data protection in Indonesia. First, the regulatory challenges. The study confirms that the existing regulation, although abundant, is still insufficient in providing comprehensive privacy and protection principles. The target groups for the existing regulations are also quite specific, with more articles and mechanisms specifically defined only for estps. There are vague and ambiguous notions for individuals and the public sector as legal subjects, creating an unclear understanding among stakeholders. Business sectors, especially big companies, including the Electronic System and Transaction Providers (ESTPs), have their own policies related to data protection. They refer to the European GDPR (General Data Protection Regulation) or the Singaporean PDPA (Personal Data Protection Act) as these two are the most comprehensive laws there are globally. Some start-ups also have their own personal data protection policies, although they seem to limit the scope of personal data protection to consent for data collection.

The second challenge is the institutional challenge. It is apparent from the cases discussed that government officials and law enforcers still lack awareness around existing regulation, let alone in implementing them. With no single regulator for data protection available, the settlement of alleged data breach and misuse cases are also scattered in various government institutions. For big companies, there is no significant institutional challenge in the existing regulations partly because they have followed a more advanced global regulation such as GDPR. For the future Data Protection Law, there is a need to establish detailed information on the criteria of a Data Protection Officer, both in government and business sector.

The third is the cultural challenge. Cultural behaviour contributed to the minimal implementation of the existing regulations. The general public doesn't acquire privacy and personal data safety as an inherent part of their citizens' rights. Therefore, there were very minimal reports of personal data misuse and breach although citizens know that their data is being traded massively. The existing regulations are also not being communicated

thoroughly, making it difficult for citizens to understand the importance of it and how they can benefit. There is an urgent need to spread, disseminate, and increase the awareness and understanding of the importance of personal data to citizens. Government, business sector, and civil society organisations should all take part in this process. Understanding the cultural background is also important to construct culture-sensitive implementation strategies for the future Data Protection Law.

Despite the challenges, there are opportunities for implementing better data protection regulations in the future. During the drafting of the future Data Protection Law, the government involved stakeholders from business sectors, other regulators, and civil society organisations in the process. They opened room for discussion and provided time for the stakeholders to give feedback. This continuous process could not only lead to a comprehensive data protection legal framework that benefits all stakeholders, but also educate those who are involved in the process.

Context

In 2018, the number of Internet users recorded in Indonesia was 171,17 million – that means 64,8% of the total population is online (APJII and Polling Indonesia, 2019). The same report highlights the highest internet penetration amongst youth aged 15-19th (91%) and young-adults aged 20-24 years (88,5%); while the lowest penetration amongst elderly aged 60-64 (16,2%) and above 65 years old (8,5%).

Although being the highest in internet penetration, young people are still lagging behind in terms of privacy awareness and data protection. A report from Web Foundation on privacy awareness in social media found that the youth in Indonesia have typical views of privacy and a low awareness of personal data protection (Canares, 2018). That being said, those that are less tech-savvy are probably even more vulnerable to privacy risks and data protection violation.

The discussion of privacy and personal data protection has increased in the past two years, especially since Facebook revealed that the personal information of Indonesian Facebook users could have been acquired by Cambridge Analytica[1]. Since then, citizens of Indonesia have questioned the protection of their personal data. Indonesia is one of the few countries in Southeast Asia that lacks an adequate legal framework on data protection (World Wide Web Foundation, 2017; GSMA, 2018). This lack of protection has led to the increase in cases of alleged personal data breach or misuse; such as the trade of bank customers and credit

[1] To solve the case, the government issued a warning letter to Facebook Indonesia but no further actions were conducted. See https://www.thejakartapost.com/life/2018/04/06/facebook-faces-indonesian-police-investigation-over-data-breach.html

card holders data[2], the spreading of customers' IDs in debt collection process[3], to the daily targeted-text messages received by individual offering products and services like loans and credits.

Data protection regulations in Indonesia are currently sporadic and limited to certain sectors, with 30 regulations identified to have clauses related to data protection (Djafar et al., 2016). There are three main legal frameworks that are deemed to be the existing core regulations related to personal data protection. Those are the Law No. 11/2008 amended by Law No. 19/2016 on Electronic Transaction, Government Regulation No. 82/2012 on Electronic System and Transactions Providers, and Ministry of Communication and Information (MOCI) Regulation No. 20/2016 on Personal Data Protection in Electronic System.

This year, the government is continuing the process of passing the Personal Data Protection Bill that provides more comprehensive principles on personal data protection that can be used across sectors. The Bill also detailed the governance of data protection such as the obligation of a data protection officer, data controller, and data protection authority, as well as mentioning the need for an independent organisation that handles data protection governance. Although there are three legal frameworks, the personal data principles in Indonesia are still far from adequate. Furthermore, cases and news on data breach and personal data misuse are still increasing.

It is then important to understand the challenges in the implementation process of the existing regulations and to identify strategies that can be improved for the implementation of the future Personal Data Protection Law.

Objectives and Methodology

This study explores the implementation of the existing regulations on personal data protection and identifies strategies from the government, business sector, and civil society organisations in complying to the existing regulation.

The questions that we addressed are:

1. What are the challenges in the implementation of the existing regulations on data protection?
2. What strategies will the public use to comply with the future personal data protection Law?

[2] See https://www.thejakartapost.com/news/2019/05/14/bank-customers-personal-data-sold-to-credit-card-salespeople-kompas-investigation.html

[3] See https://www.thejakartapost.com/news/2019/08/05/where-is-privacy-personal-data-on-spreading-spree-in-indonesia.html

The study made use of qualitative approaches with a desk study and interviews of key informants as the instruments. The key informants are the government officials, representatives from civil society organizations that advocate and work with personal data protection cases, and private sector actors who actively participate in the discussion of personal data protection issues in Indonesia. A snowball sampling approach was also applied to gain more perspective from various informants. A total of 10 informants were consulted.

Interview transcripts were subjected to descriptive analysis while results from the interviews were coded to identify common themes and patterns regarding the research questions. The main areas for discussion in the interviews were the challenges in the existing legal framework related to personal data protection, the strategies to comply with the existing legal framework, and strategies to better implement as well as comply to the future personal data protection legal framework in Indonesia.

The study is limited in coverage as it only focuses on the implementation process of the existing data protection legal framework and does not provide in-depth discussion on each of the articles in the regulations. The framework used in this research is based on the three variables of policy implementation framework (Material, Structural, and Contextual) from Sabatier and Mazmanian (1983). The three variables were chosen as it represents the focus analysis of this study: the legal framework, the implementing actors, and the social conditions.

The material variables analyse the legal framework from the technical difficulties, the diversity of the target group, and the extent of behaviour change required by the regulation. Structural variables include the focus on the institutional and implementing actors by observing the readiness of implementing organisations, the availability and capacities of implementing resources, as well as the accountability mechanism process. The contextual variables examine the social conditions by looking at the awareness of public and their readiness and support.

Existing legal framework for personal data protection in Indonesia

"The existing regulations are focusing more on the obligation of electronic system providers that collect, process, and use personal data; but lacking the details of data owner's rights and who is responsible to protect these rights."

- Human rights activist, interview, May 2019

There are three main regulations that discuss personal data in Indonesia: the EIT Law No. 11/2008 amended by Law No. 19/2016, Presidential Regulation No. 82/2012 on Electronic System and Transactions Providers, and MOCI Regulation No. 20/2016 as the implementing regulation of the Government Regulation No. 82/2012 on Electronic System and Transactions Providers (ESTP). According to this government regulation, ESTP is any person, government institutions, business entity, or community that provides, manages and/or operates an electronic system, either individually or collectively, to electronic system users for its own or another party's interests.

MOCI Regulation No. 20/2016 is the latest and most detailed as it provides a definition of personal data, details the obligations on electronic system providers related to personal data use and protection, as well as providing a mechanism for sanction and dispute settlement on personal data misuse and breach.

Law/Regulation	**Articles related to personal data**	**Scope**	**Legal Subject**	**Accountability mechanism**
Law No. 11/2008 amended by Law No. 19/2016 on Electronic Transaction	Article 26: "except otherwise regulated in another regulation, the use of information related to personal data in electronic media should be conducted based on consent"	Processing, transmission, and sharing of personal data in electronic system	Individual, companies	None related specifically to personal data; but criminal and financial sanctions available for the misuse of personal data for defamation or extortion in electronic document and transaction.
Government Regulation No. 82/2012 on Electronic System and Transactions Providers	"personal data is certain individual data that is stored, maintained, and its confidentiality is protected by the ESTP"	Collection, management, and processing of personal data in electronic system	Individuals, state institutions, and business entity	Obliges ESTP to protect personal data, obtain consent for any use of personal data,and to provide notice in cases of personal data protection failure

Ministry of Communication and Information Regulation No. 20/2016	"Personal data is certain individual data that is stored, maintained, and its confidentiality is protected." "Certain individual data is any accurate and concrete information which attached and can be identified directly or to personal data owner"	Acquisition, collection, processing, storage, display, announcement, transfer, sharing, and annihilation of personal data in electronic system	Individual, state institutions, business entity, or civil society that operate and/or use electronic system	Administrative sanction is imposed based on complaints. Dispute will firstly be addressed through non-litigation settlement. A civil lawsuit can be submitted upon the failure of non-litigation settlement.

Table 1. Existing legal frameworks related to personal data

Law No. 11/2008 and Law No. 19/2016 (amendment) on Electronic and Information Transaction

Article 26 of the EIT Law No. 11/2018, prohibits the use and transfer of personal data without consent of the individual. It also states that individuals can file a complaint and request for financial compensation if they feel that their personal data is being transferred without consent. The amendment of the Law obligated the Electronic System and Transactions Providers (ESTP) to remove irrelevant electronic information or document based on the request of the data owner through a court decision; and to provide a mechanism to do so. The Law does not discuss the comprehensive definition and scope of personal data; and there is no information on the authority responsible to protect the rights of data owners.

Government Regulation No. 82/2012 on Electronic System and Transactions Providers[4]

This regulation focuses on the obligations of ESTP, more specifically by regulating the use and location of data centre. The clause related to personal data is in one of the obligations of Electronic System and Transactions Providers where they are obliged to protect its users' personal data. The regulation also obliges ESTP to notify users in cases of personal data

[4] This regulation is currently under revision.

protection failure. Like the EIT Law, this regulation also does not provide a clear definition and scope of personal data.

MOCI Regulation No. 20/2016 on Personal Data Protection in Electronic System

This latest regulation provides a more detailed definition of personal data. There are two layers of personal data definitions. The first and general one stated that personal data is "certain individual data which veracity is recorded, sustained, and maintained and confidentiality is protected." It then further defines certain individual data as "any accurate and concrete information which is identifiable and directly or indirectly attached to the personal data owner". The regulation also further detailed the provision of notice in cases of personal data protection failure by the ESTP; a clause that is not available in the Government Regulation No. 82/2012. The rights of personal data owners are also available in the regulation, although at a minimum.

Synthesis

The three regulations above focus on personal data processed through electronic systems only; while the non-electronic means of personal data collection, processing, and use, still refer to regulations in each sector. For example, the collection, processing, and transmission of personal data in the financial sector refer to Financial Service Authority Regulation No. 77/2016 on Information-Technology based Money Lending Services and Financial Service Authority Regulation No. 13/2018 on Digital Financial Innovation. These regulations do not refer to the MOCI regulation and therefore have their own legal subject and scope.

The MOCI regulation limits the period of personal data retention to 5 years minimum. In government institutions, archiving and the retention of data, including personal data, is based on the Archive Law No. 43/2009; while business sector usually has their own policy on the data retention period. In terms of data transfer and sharing, all three regulations rely on written consent that should be provided in Bahasa Indonesia, but no further information on how the consent should be obtained.

Although the MOCI regulation provides details on personal data protection, the level of regulation is insufficient to have an impactful enforcement. Ministerial regulation only allows to impose administrative sanction in terms of data protection misuse or failure. The EIT Law has strong sanctions for the misuse of electronic information (including personal data), but then again, this Law does not have a clear definition of personal data and therefore difficult to obtain sufficient evidence to bring the case to court (Greenleaf, 2017).

"If you asked whether we try to comply with the existing regulations, of course we do. But whether we make it [complying to the regulations] a priority, I don't think so... because it is still not comprehensive. We treated the MOCI regulation more as a guideline; while we refer most of our [data protection] policies to GDPR and PDPA."

- Legal officer, business sector, interview, June 2019

The insufficient level of ministry regulation also makes it difficult to expect a behavioural change required by the regulation. Government institutions are still adhering to their sectoral Law rather than the MOCI Regulation. The business sector is also still referring to GDPR and PDPA as the main source for developing their data protection policies.

Institutional challenges and accountability process

Institutional challenges

"The officials in government institution are mostly still unaware of the existence of MOCI Regulation on Personal Data Protection in Electronic System... They don't understand that they are part of the legal subject of the regulation, and that they are responsible to protect citizens' personal data collected and processed by them."

- State official, Interview, July 2019

Two main institutional challenges within the government were observed in the implementation of the existing regulations:

1. Overlap of responsibilities. Since there is no single regulator responsible for personal data protection and governance, cases related to personal data governance are still being handled based on the sector. For example, for the misuse of personal data by ESTP, the Directorate General of ESTP Monitoring in the Ministry of Communication and Information will be the responsible regulator. The misuse of personal data related to financial sector will be handled by the Financial Service Authority, and the Ministry of Health is responsible for personal data misuse related to medical records.

2. Lack of knowledge, capacities, and capabilities of regulators. Most state officials are still not aware that they are processing citizens' data, and there are no specific internal policies to obtain consent in processing citizens' data. Since the existing regulations focus mostly on ESTPs, state officials still feel that they are not bound by the regulation, although it is clearly stated in the MOCI Regulation No. 20/2016 that state officials are part of the legal subject if they processed personal data in an electronic system.

"Education [on personal data] is important, not only for the citizens, not only for data owners, but most importantly for the law enforcer, for the state officials. I don't think it [personal data protection] is something that they are already aware of."

- Representative from Telecommunication Company, Interview, May 2019

The Ministry of Communication and Information have capacity building programmes on data protection and they regularly send state officials from different institutions to participate in workshops, trainings, and certification programmes related to data protection. The attempts to improve the capacity and knowledge of state officials are available, but still very limited.

The business sector has more advanced institutional capacities. Three out of four companies interviewed admit that they already have a dedicated officer that handles personal data protection. The officer is usually integrated with Legal and Compliance Department or as part of the IT Department. All companies that were interviewed also have internal capacity building programmes to improve the officers' knowledge and skills in data governance and personal data protection. Business associations also create guidelines for personal data protection. For example, the Indonesian Fintech Lender Association (AFPI) created guidelines that discuss the obligation to obey to the existing regulation on personal data protection, and the eligible debt collection procedure for online lending companies.

Accountability process

"The implementation of sanction [of personal data breach or misuse] is still difficult... It is not clear who has the authority to confirm, investigate, and make decisions on the incident of data breach; is it the government? Who in the government? Which institution?... ESTPs also didn't notice their users in cases of data protection failure [as

mandated in Government Regulation No. 82/2012]; citizens also rarely file a complaint for personal data misuse... So it [the implementation of sanction] is not working well."

- Civic Lawyer, interview, July, 2019

The weak sanction, the absence of an independent investigator, the unclear and overlap of authorities in handling personal data misuse leads to a toothless accountability process. Currently, reports of personal data misuse are mostly being received by Ministry of Communication and Information, but they do not have the authority to impose sanctions and only act as an intermediary. The Ministry then forwards the case to the Attorney Office of Indonesia (for cases related to defamation) or to the relevant sectoral Ministry. Our respondents from human rights organisation, state officials, and representatives of business sector agree that there is always insufficient evidence to process a lawsuit related to personal data misuse. The weak sanction is also as a result of the lack of capacities in the implementing resources, in this case, government institutions and law enforcement.

"What is concerning is when the State itself does several partnerships with third parties related to our [citizens] personal data. Although technically there is no personal data that is being transferred or shared, but that is not the main point. The point is in transparency, accountability, and citizens' rights to their personal data, how do they [the state] protect it [citizens' data]... So it's not about protecting the data, but protecting citizens' rights of their personal data."

- Digital Literacy worker, interview, July 2019

Government institutions that collect and use citizens data treated personal data similar to regular data. Since the regulations do not detail any mechanism for personal data misuse conducted by the government, the accountability process of how personal data is stored, who has access to it, and the mechanism for data sharing, if any, is never disclosed.

Social and cultural implications

"What happened here [related to personal data] is people voluntarily and happily share their personal data. If you

look at Instagram, for example, the way I see it, on Instagram we share data and information that we want people to know. It is slightly different with the kind of personal data protection, different with the personal data that I want to secure like phone number, ID number. But people can't differentiate between the two [kinds of personal data]... It is hard for us [the company] to protect personal data of people who do not even protect their data."

- Public policy officer, business sector, interview, June 2019

Citizens are the most vulnerable actors in the absence of a comprehensive data protection regulation In Indonesia. However, most citizens are still not familiar with the basic concept of privacy and personal data protection. Personal data is yet to be seen as part of personal property and therefore is not consciously protected. This lack of awareness relates closely with the cultural background that has long been studied as a crucial part of privacy regulatory mechanism (Altman, 1977; Li, 2011; Trepte et al., 2017). Indonesia seems to lack the attention to the cultural characteristics of its citizens, both in constructing and implementing the regulations.

Communicating privacy and personal data to the public is arduous. Most citizens and organisations still perceive privacy not as a human right but more as 'security' – this then leads to fear of going back to the 'New Order' era where everything is closed/protected by the government. With data protection regulations, citizens fear that the government will close the information that is now open to the public. Furthermore, looking at the general online behaviour of the citizens, only a small part of citizens are aware of the privacy risks, while most citizens still neglect the privacy risks to acquire benefits from many kinds of services that they got online. For example, the risk of privacy intrusion in online lending is often neglected, especially by female users, due to the expected benefits such as being able to apply for credit loans without the approval of their partner.

"...These women [online lending users] don't care about the [privacy] risks... what matters is that now they can apply for loans, without the approval from their husband, using their own mobile phone and account. And that makes them feel more independent. You may say that this [online lending] practice is risky. But risky for whom? For them, the benefits exceed the risks."

- Civil society representative, interview, July 2019

Although many cases and stories about privacy and personal data intrusion are in the news, it is still an unfamiliar issue and only touches upon the most well informed. There needs to be a structured and massive movement to spread awareness through different channels, such as educational systems and better business practices. In the subject where citizens are the most vulnerable and have lack of awareness, the government should play its role in providing a comprehensive protection.

People that we consulted expected the future Data Protection Law to not only regulate, but also educate its citizens about the importance of data protection. However, since the most comprehensive regulation available now is GDPR, most of the frameworks in the Bill are referring to the Regulation.

"...the article about DPO [in the Bill], it is only like a copy-paste version from GDPR. Yes, maybe having a DPO is one of the indicators that we have an adequate personal data regulation, but we should also think about the process [of drafting the regulation]. They [the EU] are far more advanced than we are, the people have a good understanding of privacy. Not everything that applies there can also be constructed here."

- State Official, interview, July 2019

Due to the differences in cultural characteristics, referring the aspect to GDPR maybe not always be the best option. For example, GDPR has advanced articles on privacy-by-design; and it focuses on the obligation of data processor and controllers. This is because the citizens of Europe have different levels of understanding of privacy (Trepte et al., 2017). Furthermore, in the EU, the Directives on data protection have existed since 1995; the people in the EU have had ample time to learn about data protection in the lead up to when the GDPR was discussed in 2014 and enacted in 2018. Although this ample time does not guarantee that they have better privacy awareness, the efforts to maintain privacy have been going on since before the GDPR was enacted. Indonesia still has to juggle between increasing the awareness and educating citizens on privacy and data protection, constructing comprehensive principles on personal data protection legal framework, while maintaining its growing digital economy at the same time. In addition to GDPR, looking at the practices from neighbouring countries that already have data protection legal framework, such as the Philippines and Singapore, may be useful considering the similar cultural backgrounds.

Recommendations

"The discussion and narrative of personal data protection [in Indonesia] is now being reduced to privacy breach [only], whereas it should be understood as an inherent part of citizens' rights. We [as citizens] have the rights to be protected by the state, including our personal data."

- Representative from MOCI, Interview, July 2019

- As long as there is no comprehensive regulation on data protection, clear guidelines on data collection and use should be in place. A rigid legal framework might be less useful considering the lack of understanding about privacy and data protection as well as the readiness level of stakeholders that will be affected. Hence, providing a series of guidelines on how to protect personal data and how to collect and use them, might be more useful. These guidelines can be used not only by internal government institutions or big companies, but also by micro-small enterprise, growing start-ups, civil society organisations, and citizens at large.

- Due to the ingrained sectoral work among government institutions, a single-independent body that is responsible for data protection is required. The model of the body should be discussed further considering internal factors such as the function, the possible structure, and the state budget available to establish such a body. As an alternative, this independent body could be suggested through Parliament as one of the mandates of the future Data Protection Law. The establishment process of this body should be open and closely monitored by all stakeholders.

- In terms of sanction scope, if administrative sanction alone is not working well, a gradation of financial sanction could be explored. The gradation could be based on (i) whether the legal subject is individual or organisations; (ii) the size of enterprise/organisation; or (iii) the quantities of personal data that they processed. Furthermore, there should be a clear remedy mechanism for those who are affected by the personal data misuse and breach.

- A regulatory sandbox model - a mechanism where regulation is developed in parallel with the changing business model and innovation - can be implemented for the implementation of the future Data Protection Law. The multi-stakeholders' discussion that has been ongoing in the drafting process of the Bill could be continued as a sandbox, adding other important actors along the way. The benefits of this practice is that it can tackle two main uncertainties at the same time (Centre

for Information Policy Leadership, 2019) – uncertainties of the growing digital innovation, and uncertainties of the regulations. It can become a learning process for the enforcement of the Law whilst maintaining the growing innovative digital ecosystem.

- Strengthening and harmonising citizens' movement on privacy and personal data literacy from the grassroot level. These movements can then add a cultural dimension in the implementation of data protection regulation and can become a solution to address the gap of privacy culture and knowledge among citizens. Adding a cultural dimension in the construction and implementation of regulations is important to make it more culture-sensitive.

A large amount of research dives into the privacy principles and values that should be incorporated in a legal framework. However, not many discuss the challenges in the implementation of a personal data protection legal framework, especially in the non-EU and US context. This study only observed a small part of the subject and more studies are still needed to come up with striking solutions to address the challenges in the implementation of personal data protection legal framework around the world.

References

Altman, I. (1977) Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*. [Online] 3366–84.

APJII & Polling Indonesia (2019) *Penetrasi & Profil Perilaku Pengguna Internet Indonesia: Survei 2018*.

Canares, M. (2018) *Online Privacy: Will they Care? Teenagers Use of Social media and their Understanding of Privacy Issues in Developing Countries*. [online]. Available from: https://webfoundation.org/docs/2018/08/WebFoundationSocialMediaPrivacyReport_Screen.pdf.

Centre for Information Policy Leadership (2019) *Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice*. [online]. Available from: https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_on_regulatory_sandboxes_in_data_protection_-_constructive_engagement_and_innovative_regulation_in_practice__8_march_2019_.pdf.

Djafar, W. et al. (2016) *Protection of Personal Data in Indonesia: A Proposal for Policy Institutionalisation from the Human Rights Perspective*. [online]. Available from: https://elsam.or.id/protection-of-personal-data-in-indonesia-a-proposal-for-policy-institutionalisation-for-the-human-rights-perspective/.

Greenleaf, G. (2017) *Global Data Privacy Laws 2017: 120 National Data Privacy Laws, Including Indonesia and Turkey*. [online]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2992986.

GSMA (2018) *Regional Privacy Framework and Cross-Border Data Flows: How ASEAN and APEC can Protect Data and Drive Innovation*. [online]. Available from: https://www.gsma.com/publicpolicy/wp-content/uploads/2018/09/GSMA-Regional-Privacy-Frameworks-and-Cross-Border-Data-Flows_Full-Report_Sept-2018.pdf.

Li, Y. (2011) Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*. [Online] 28 (28), . [online]. Available from: https://aisel.aisnet.org/cais/vol28/iss1/28.

Sabatier, P. A. & Mazmanian, D. A. (1983) *Implementation and public policy*. Scott, Foresman public policy analysis and management series. Glenview, Ill: Scott, Foresman.

Trepte, S. et al. (2017) A Cross-Cultural Perspective on the Privacy Calculus. *Social Media + Society*. [Online] (January-March), 1–13. [online]. Available from: journals.sagepub.com/home/sms.

World Wide Web Foundation (2017) *Personal Data: An overview of low and middle-income countries*. [online]. Available from: http://webfoundation.org/docs/2017/07/PersonalData_Report_WF.pdf.

Open Data Lab Jakarta

labs.webfoundation.org
@ODLabJkt
info@labs.webfoundation.org

World Wide Web Foundation

webfoundation.org
@webfoundation
contact@webfoundation.org