

Suleiman, Ajisatria; Audrine, Pingkan; Dewaranu, Thomas

Research Report

Co-regulation in protecting personal data: The role of industry associations as potential self-regulatory organizations

Policy Paper, No. 50

Provided in Cooperation with:

Center for Indonesian Policy Studies (CIPS), Jakarta

Suggested Citation: Suleiman, Ajisatria; Audrine, Pingkan; Dewaranu, Thomas (2022) : Co-regulation in protecting personal data: The role of industry associations as potential self-regulatory organizations, Policy Paper, No. 50, Center for Indonesian Policy Studies (CIPS), Jakarta

This Version is available at:

<https://hdl.handle.net/10419/298413>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.



CIPS
Center for Indonesian
Policy Studies

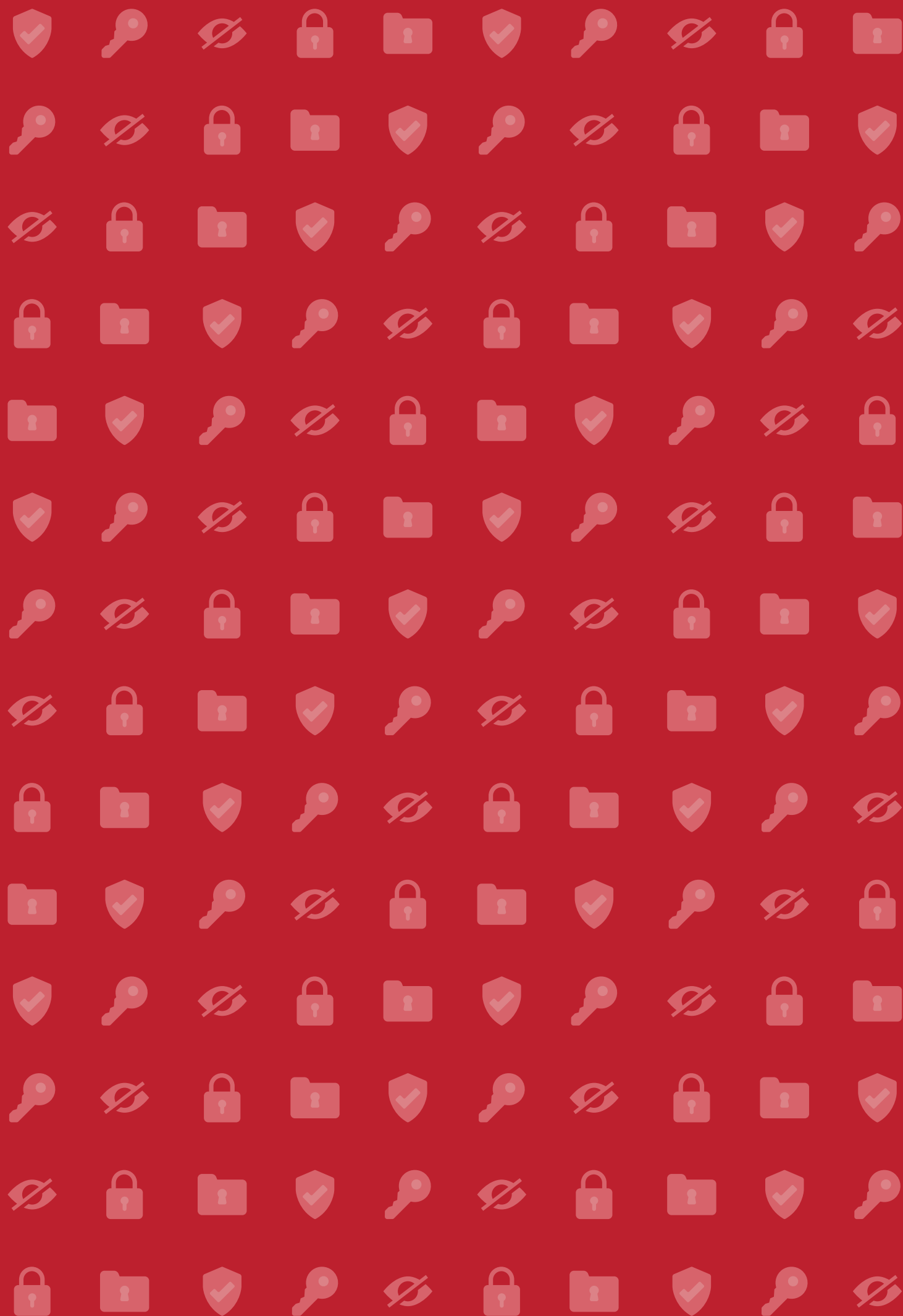
Policy Paper No. 50

Co-Regulation in Protecting Personal Data:

The Role of Industry Associations as
Potential Self-Regulatory Organizations

by Ajisatria Suleiman, Pingkan Audrine, & Thomas Dewaranu

www.cips-indonesia.org



Policy Paper No. 50

Co-Regulation in Protecting Personal Data:

The Role of Industry Associations as Potential Self-Regulatory Organizations

Authors:

Ajisatria Suleiman, Pingkan Audrine, & Thomas Dewaranu
(Center for Indonesian Policy Studies)

Jakarta, Indonesia

July, 2022

Copyrights © 2022 by Center for Indonesian Policy Studies

Acknowledgement:



We would like to thank the Center for International Private Enterprise for their support with this publication.

The authors would like to thank Felippa Amanta for her tremendous assistance in this paper.

Cover:

tete_escape/Freepik.com

CONTENT

Table of contents	5
List of Tables	6
List of Figures	6
Glossary	7
Executive Summary	9
Introduction	10
Explaining the Gap: Why Co-Regulation in Personal Data Protection is Important	13
Industry Associations and Current Practices of Co-Regulatory Role	19
History of Co-regulation in Indonesia: Digital Economy & Financial Sector.....	19
Industry Associations and Personal Data Protection: Growing Practices in Digital Finance.....	22
AFTECH Code of Ethics on Personal Data Protection.....	23
AFPI Code of Conduct for the Responsible IT-based Lending and Borrowing Services.....	25
Enforcement of AFTECH Code of Ethics for Personal Data Protection and AFPI Joint Code of Conduct.....	26
The Next Avenue: Potential Co-Regulatory Role of Data Protection Officer (DPO) Association	29
Data Protection Officer (DPO) under PDP Bill and Other Existing Regulations.....	29
DPO Roles and Accountability.....	30
DPO Training and Certification.....	31
Different models of professional certifications.....	31
Association Membership and Ethical Role.....	33
Comparison with GDPR.....	35
DPO in Spain: Central Roles of the Data Protection Agency.....	36
Conclusions and Recommendations	37
References	40

LIST OF TABLES

Table 1. Proposed Monetary Sanctions for PDP Violation.....	17
Table 2. Sectoral Regulations that Empower Associations.....	21
Table 3. Components of AFTECH Code of Ethics for Personal Data Protection.....	24
Table 4. List of Associations Related to the Digital Economy Ecosystem and Data Protection Officer in Indonesia.....	38

LIST OF FIGURES

Figure 1. MOCI's Structure on Personal Data Protection.....	14
Figure 2. MOCI's Flow of Action When Dealing with Reported/Alleged Personal Data Breach Cases.....	15
Figure 3. PDP Related Cases or Incidents Handled by MOCI (2019-April 2021).....	16
Figure 4. Training and competency certification mechanism under the SPKN.....	32

GLOSSARY

BNSP:

National Professional Certification Agency or Badan Nasional Sertifikasi Profesi

DPO:

Data Protection Officer

EIT Law:

Law No. 11 of 2008 on Electronic Information and Transaction and its No.19/2016 Revision

ESOs:

Electronic System Operators

GDPR:

General Data Protection Regulation

IDX:

Indonesia Stock Exchange

ISP:

Internet Service Providers

KAN:

National Accreditation Committee or Komite Akreditasi Nasional

KPEI:

Indonesian Clearing and Guarantee Corporation or Kliring Penjaminan Efek Indonesia

KSEI:

Indonesian Central Securities Depository or Kustodian Sentral Efek Indonesia

LSP:

Professional Certification Agency or Lembaga Sertifikasi Profesi authorized by BNSP

MOCI:

Ministry of Communication and Informatics

MOT:

Ministry of Trade

OJK:

Financial Services Authority or Otoritas Jasa Keuangan

PDP:

Personal Data Protection

PKPA:

Special Education for Advocates or Pendidikan Khusus Profesi Advokat

PPDP:

In the draft PDP Bill, Indonesian government use the term Pejabat atau Petugas Pelindung Data Pribadi to refer to the DPO position.

SKKNI:

Indonesian National Work Competency Standard or Standar Kompetensi Kerja Nasional Indonesia

SPKN:

National Job Training System or Sistem Pelatihan Kerja Nasional is regulated by Law No. 13 of 2003 on Manpower (Labor Law) jo. Government Regulation No. 31 of 2006 on National Job Training System (GR 31/2006).

SRO:

Self-Regulatory Organization

EXECUTIVE SUMMARY

As the digital economy is growing in Indonesia at an exponential rate, there is a need to come up with a novel approach to regulating the activities and transactions happening in this space. This is especially true in the sphere of personal data protection, where massive amounts of personal data are collected, processed, and stored by various entities for various purposes. It is difficult for regulators to supervise all activities and ensure compliance with best practices within digital platforms, both in the public and private sector. A co-regulatory approach becomes a potential solution to this issue.

A co-regulatory approach in personal data protection can complement enforcement of professional and technical sector-specific standards, focus on preventative measures, and engage non-state actors in enforcement mechanisms. Unique to Indonesia, especially in financial services, industry associations have been serving in the role of “self-regulatory-organizations” that complement the supervision of regulated entities. Recently there have been precedents to expand this into digital finance, including in the event of personal data protection violations. This model can be adopted for digital platforms in the general ICT sector. Taking the opportunity of the upcoming Personal Data Protection (PDP) bill that, according to Article 55 of the Bill, would enable industry associations to implement co-regulatory activities, industry associations can develop their own sector-specific technical standards in personal data governance and can also enforce these standards through “peer enforcements”. The Government, on the other hand, will still impose regulatory oversight to ensure that these industry initiatives are implemented fairly and in line with market competition principles. Another potential avenue for co-regulation is to empower the profession of Data Protection Officer (DPO), which based on the experience in other jurisdictions, can set professional community standards for best practices in personal data protection.

INTRODUCTION

Indonesia has been exposed to an economic boom as the result of the introduction of the digital economy. The sector's Gross Merchandise Value (GMV) is predicted to reach USD 146 billion in 2025, an enormous growth from USD 40 billion in 2019 (Google, Temasek, & Bain & Company, 2021). However, the rapid innovation and development of the digital economy sector in Indonesia has not been fully supported by an equally agile regulatory framework. Such agility is needed to stimulate industry growth while providing consumers sufficient legal protection. The lack of agile regulatory framework can be seen from the absence of national laws on Personal Data Protection in the country and the outdated Consumer Protection Law No.8/1999.

Improper handling of personal data negatively affects consumers, exposing them to risks of fraud from data breaches, having their privacy rights violated, and potential exploitation. The protection of personal data is essential to privacy and security and requires the attention of and action from government, the private sector, and citizens.

A crucial backbone of the digital economy is the protection of personal data. Commercial digital platforms collect, process, and monetize personal data at a massive scale to generate revenue through advertising or by other means. Public sector agencies also collect and process data for various purposes, from public service delivery to surveillance. Improper handling of personal data negatively affects consumers, exposing them to risks of fraud from data breaches, having their privacy rights violated, and potential exploitation. The protection of personal data is essential to privacy and security and requires the attention of and action from government, the private sector, and citizens. Data protection frameworks can help foster consumer trust and increased digital adoption, which in turn can incentivize investment, competition and innovation in the Indonesian digital economy.

Within this context, there are two major regulatory challenges in this emerging sector: (i) the lack of a coherent regulatory landscape governing the digital economy—particularly on data protection; and (ii) the persistent government-centric approach to policymaking that hinders a collaborative approach in response to the emerging challenges. Data protection is a multi-stakeholder issue in digital economy.

Regarding the first challenge, as showcased by Aprilianti & Dina (2021), there are at least 14 government ministries and institutions that regulate the digital economy sector with over 60 laws and regulations in place. More than half of those laws and regulations are concerning Personal Data Protection with a sector-specific focus, for example telecommunication, electronic information and transactions, banking and finance, electronic system operators, government administration and health. However, some regulations are overlapping, and contradict each other. One example is the differences in classification of personal data under

two existing regulations: the Electronic Information and Transactions (EIT) Law No.19/2016 and the Population Administration Law No.24/2013 (Riyadi, 2021).¹ Hence, having an encompassing Personal Data Protection Law becomes more crucial in providing a comprehensive legal basis for data protection and privacy. That should also be followed by preemption to or amendments to existing laws that would otherwise have contradictory provisions about data protection.

In 2014, the Ministry of Communication and Informatics (MOCI) kick-started the drafting process of the Personal Data Protection Bill (PDP Bill) and submitted it to the government in 2020 (Karunian, 2020). Although the bill has been included in the National Legislative Agenda for 2020, 2021, and 2022, the deliberations have not concluded yet. Contrasting views between MOCI and the Members of Parliament on the Data Protection Authority provisions resulted in a stalemate up to the publishing of this research in July 2022.

Navigating the second challenge, the traditional policymaking and governance approach that revolves around command and control, also known as a top-down or state-controlled approach, may not be well-suited for the fast-evolving and highly-technical digital economy sector. A co-regulatory approach or co-regulation for the digital economy would entail continuous and broad-based multi-stakeholder input during the policymaking process and also responsibility-sharing between government and non-governmental stakeholders within the implementation and evaluation process, as have been proposed (Finck, 2017; Torfing et al., 2016; and Hepburn, 2018).

Research conducted by the Center for Indonesian Policy Studies (CIPS) have explored the costs and benefits of having a co-regulatory approach implemented in Indonesia's digital economy. The studies found that creating space for a more active role and delegation to non-governmental stakeholders in implementing digital economy policies can benefit Indonesia's digital economy to grow further, allowing more innovations and effectively addressing digital problems based on each stakeholders' capacity. For example, government can focus with the regulatory making process and its monitoring upon the implementation. Meanwhile, other major roles can be taken by businesses or industry associations in educating users through literacy programs and capacity building for digital talents to name a few (Aprilianti & Dina, 2021; Riyadi, 2021; Suleiman, 2021; and Audrine & Murwani, 2021).

This paper assesses a novel approach to co-regulation through the instrument of industry associations. The importance of business and professional associations in the digital economy is expressed in different regulations in Indonesia given their ability to self-regulate beyond regulatory curve. Article 55 of the Personal Data Protection (PDP) bill, for example, allows industry associations to develop a code of conduct for data controllers and processors in handling personal data.² The code must consider the principles of personal data protection, the limited purpose of personal data use, and the interests of the data owners. Further, the bill also stresses that the code of conduct must not contradict the bill while also guaranteeing at least

¹ According to Population Administration Law No. 24/2013, Personal Data is certain individual data which is stored, cared for, and is kept true and protected by confidentiality. There is no further categorization of what belongs to this definition. Meanwhile, for the EIT law the categorization is quite extensive without specific provisions on personal data. Instead, EIT Law use the term of electronic data which is defined as one or a set of data that include but not limited to writing, sound, pictures, maps, designs, photographs, electronic data interchange (EDI), electronic mail (e-mail), telegram, telex, telecopy or the like, letters, signs, numbers, access codes, symbols, or processed perforations that have meaning or can be understood by people.

² The PDP bill draft used in this paper is the January 2020 version. Available at <https://www.hukumonline.com/pusatdata/detail/lt561f74edf3260/ruu-pelindungan-data-pribadi-tahun-2020/document>

the same level of protection standards set by the bill. However, industries, sometimes through associations, have engaged in data protection measures in different digital sectors by referring to different sectoral regulations. These are evident in the digital finance sector, where industry associations are already acting as SROs to enforce technical standards.

Given that the approach is unique to Indonesia, it becomes necessary to look into these collaborative regulatory practices and see how they would fit with the general data governance enforcement. In particular, the paper will cover two types of associations: business associations and professional associations. According to the Organization of Economic Cooperation and Development, a business/ industry association is an organization where companies that belong into the same sector can coordinate collective efforts and are able to build cooperation based on the shared interests within that particular industry (Hepburn, 2018). The other type is a professional association, which is a legal entity that provides avenues for individuals who have the same professional skills and vision in developing professions' practices. It has the responsibility to cultivate, protect, and develop professional skills for its members (Susanto, n.d.). In the case of personal data protection, the growing role of Data Protection Officer (DPO) as a profession has propelled the influence of DPO association as a key actor in personal data protection governance.

EXPLAINING THE GAP: WHY CO-REGULATION IN PERSONAL DATA PROTECTION IS IMPORTANT

Personal data protection lies at the core of the digital economy, especially in Indonesia, where it is still being developed through various legislative and regulatory measures. Digital platforms, also known as, Electronic System Operators (ESOs) in Indonesia, exist both in the public and private sector, and increasingly generate, collect, and process data of individuals. Throughout the years, there have been major incidents involving personal data breaches where hackers attacked and stole data from government databases. The two biggest cases are data breaches in General Election Commission (*Komisi Pemilihan Umum* or KPU) and Social Security Administrator for Health (*Badan Penyelenggara Jaminan Sosial Kesehatan* or BPJS Kesehatan). Besides government agencies, online marketplaces, like Tokopedia and Bukalapak, and user-generated content platforms, like Facebook, were also victims of data breaches.

A strong data protection framework will enable enforcement mechanisms against illegal perpetrators such as hackers, scammers, and other cybercriminals; but also install a system of legal accountability of such ESOs to ensure they impose appropriate measures to identify whether they are liable to the breach, or implement sufficient measures to prevent such breaches from happening in the future. In the long run, data protection frameworks help foster consumer trust and increased digital usage, which in turn can incentivize investment, competition and innovation in the Indonesian digital economy.

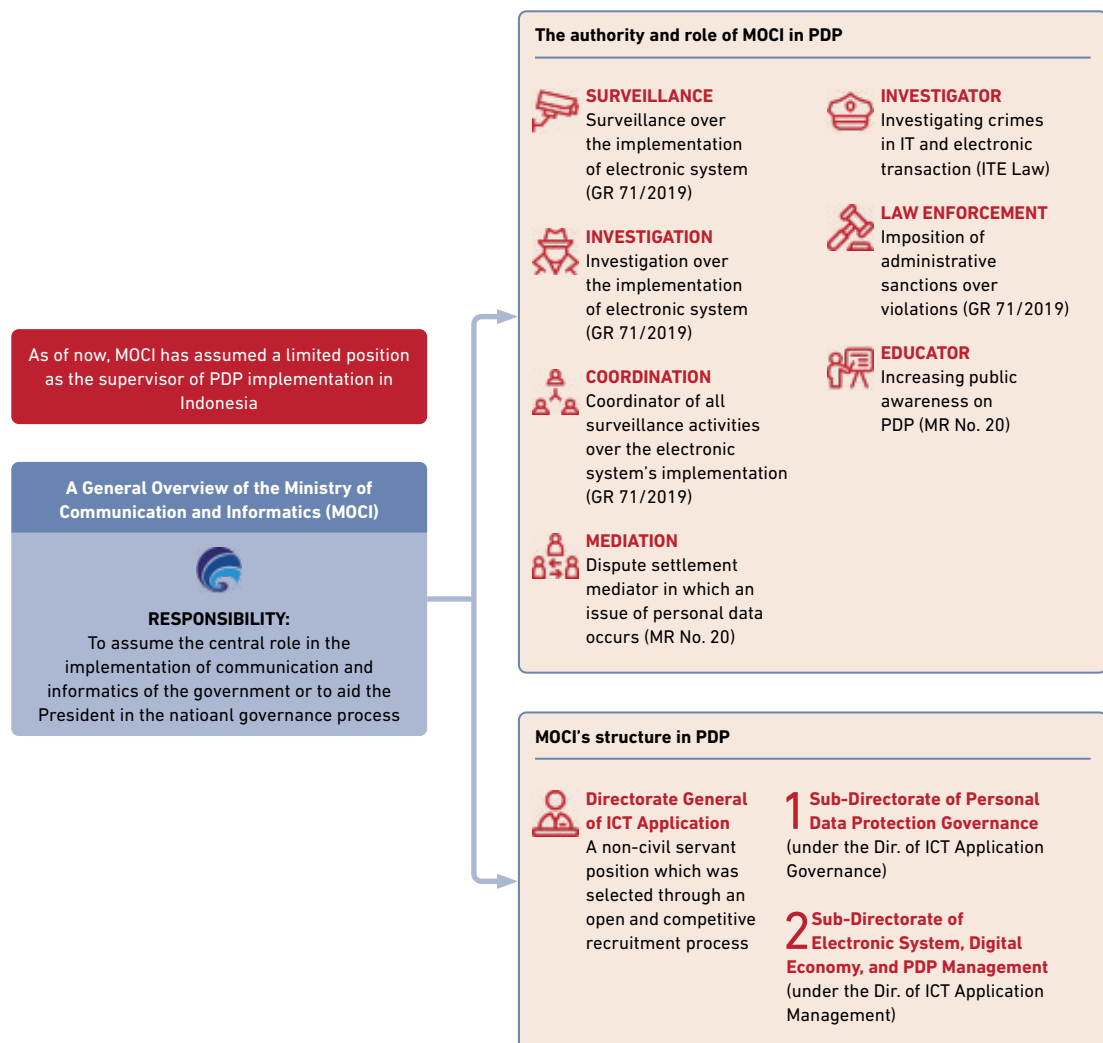
While several regulations are already in place at the technical level such as the Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (GR 71/2019) and at the sector-specific level within the financial services or healthcare, another legislative-level regulation is currently in the making under the parliamentary deliberation of the PDP Bill. Amidst this regulatory framework the private sector has an emerging role to create rules and ensure compliance. The private sector arguably has an alignment of incentives to uphold personal data principles in order to maintain the trust of its consumers. This fosters a potential avenue for co-regulation to flourish.

The current regulatory framework for personal data protection employs a top-down approach with the MOCI as the main regulator and administrator. Pursuant to GR No.71/2019 and its implementation regulation MOCI Regulation No.5/2020, MOCI has the authority to require all platforms—known as Electronic System Organizers (ESOs) or *Penyelenggara Sistem Elektronik*—to register in MOCI via the Online Single Submission (OSS) system prior to commencing its operations. The registration requirement applies to both (a) domestic ESOs (Indonesian legal entities) and (b) foreign ESOs firms that provide services in the Indonesian territory, do business in Indonesia or provide services that are being used in Indonesia. MOCI can then impose sanctions on ESOs that fail to comply with MOCI requirements, including on personal data protection. The sanctions range from a warning letter, monetary penalties, revocation of ESO registration, and

In the long run, data protection frameworks help foster consumer trust and increased digital usage, which in turn can incentivize investment, competition and innovation in the Indonesian digital economy.

access cut-off that will affect ESO operation in Indonesia. The last sanction means that ESO will no longer be accessible in Indonesian market. MOCI has the authority to instruct Internet Service Providers (ISPs) to cut-off access to ESOs whose registration has been revoked.

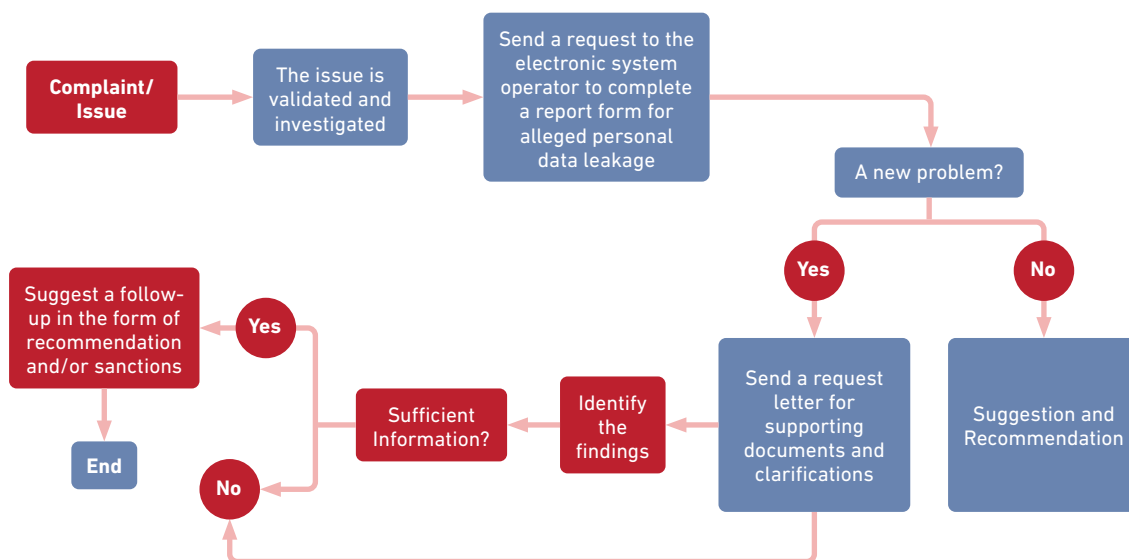
Figure 1.
MOCI's Structure on Personal Data Protection



Sources: Directorate General of ICT Applications of MOCI (2021)

MOCI handles complaints from users or any third party over allegations of a personal data breach, which then will be followed up by MOCI to the relevant ESOs. In addition, MOCI also can perform investigation, validation, and clarification to determine actions, and sanctions if there is indeed a violation.

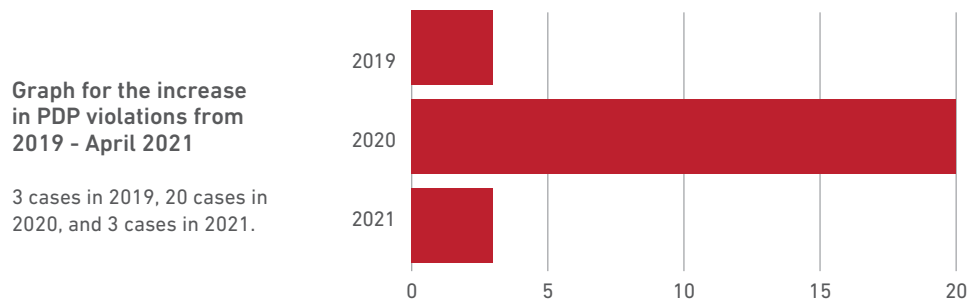
Figure 2.
MOCI's Flow of Action When Dealing with Reported/
Alleged Personal Data Breach Cases



Sources: Directorate General of ICT Applications of MOCI (2021)

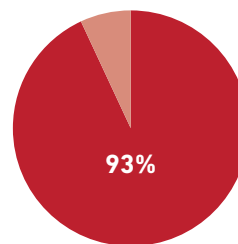
Equipped with these resources and systems in place, MOCI has been carrying out its mandate to supervise personal data protection. Based on MOCI's data, 93% of cases or incidents handled by them were personal data leakages, and 92% of which were due to cyber security incidents. E-commerce companies dominated the incidents with 39.3%, followed by public institutions (14,3%). From 2019 to 2022, the Directorate General of Application Informatics recorded 47 cybercrime cases, consisting of cyber-attacks by hackers and data leakages. MOCI took further steps in taking 16 cases for sanctions recommendation, 10 cases are still under investigations.

Figure 3.
PDP Related Cases or Incidents Handled by MOCI (2019-April 2021)



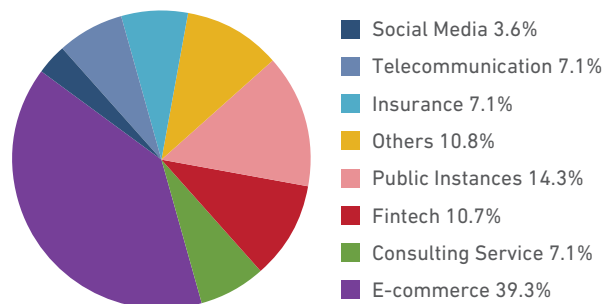
93% of the cases received are personal data leakage issues and the other 7% violate other PDP principles.

92% of personal data leakage issues are caused by cyber incidents.



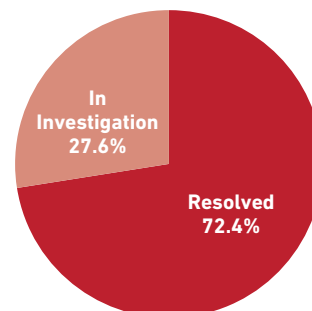
Classification of the electronic system's implementation that violates PDP

E-commerce is the top violator of PDP in the period time between 2019 - May 2021



The conduct towards Personal Data Protection violations

From 29 cases of personal data leakage issues that occurred since 2019, there have been 21 resolved cases.



Sources: Directorate General of ICT Applications of MOCI (2021)

More recently, MOCI's effort to strengthen its supervisory authority is complemented by a plan to also impose monetary fines over the personal data breach. MOCI is preparing a draft regulation that lists seven main categories of personal data breaches, each with further detailed violations. Each violation is assigned specific point amount, and each point is equal to IDR 100,000 (Table 1). MOCI is also developing a "weight" based on the size of ESOs, in which case the micro-sized online businesses will only receive 25% of the penalty, small-sized 50%, medium-sized 75%, and large enterprises 100%, respectively.

Table 1.
Proposed Monetary Sanctions for PDP Violation

Types of Violation	Points
1) The collection of Personal Data is not limited and specific, lawful, just, and conducted upon the owner's knowledge and consent	
a) There is no specific goal and limitation established	1.000
b) There is no legal framework that addresses the issue of personal data processing	1.000
c) The existing legal framework for personal data processing is not in accordance with its initial goal	800
d) There is no notice pertaining to the personal data processing in the permission request to the data's owner	50
2) The Personal Data processing is not in accordance with its goals	
a) There exists one or more goals for personal data processing, yet the personal data collected is not in accordance with the established goals	400
b) There exists one or more goals for personal data processing, but the process is not in accordance with the established goals	700
c) In a case where additional goals are present, additional analysis to determine whether the additional goals conform with the initial goal is not conducted	200
3) The Personal Data processing does not guarantee the rights of its owner	800
4) The Personal Data processing is not carried out in accurate, complete, factual, up-to-date, and accountable manner, as well as disregarding the goal of the processing	
a) The Personal Data processing is carried out in an inaccurate, incomplete, misleading, and not up-to-date manner	800
b) The Personal Data processing cannot be held accountable	1.000
5) The Personal Data processing is carried out without any consideration to the safety of its owner from Personal Data loss, misuse, unlawful access, alteration, and impairment	
a) Personal data loss	10.000
b) Personal data abuse	5.000
c) Unlawful access to personal data	5.000
d) Unlawful alteration and impairment of personal data	10.000
6) The Personal Data processing is carried out without any notice pertaining to its goal of collection, processing activity, and failure in Personal Data Protection	1.500
7) Personal Data is not omitted or erased, except in a retention period that is in accordance with the obligations stipulated in statutory regulations	
a) The absence of provisions for the retention period	50
b) The lack of procedure and/or provisions on the omission of Personal Data after the retention period elapses	150

Sources: Directorate General of ICT Applications of MOCI (2022)

While MOCI deserves praise for its effort to assert its authority as personal data supervisor through diverse regulatory tools (from ESO registration, investigation, monetary fines, and access cut-off), the current approaches are still missing the element of interaction with the private sector.

First, there is no systematic effort to improve the quality of human resources to deal with privacy and security issues. Key to privacy and security best practices is a solid talent of professionals that will be the safeguard of platforms from data breaches or privacy violations. In order to do so, there needs to be continuous professional education and executive learning programs for the relevant professionals. A similar model can be found in the financial sector, whereby continuous executive education for certain types of expertise, such as risk management, is mandatory.

Second, preventative measures are still lacking. As MOCI data suggests, 93% of incidents were results of the data breaches that already happened. Preventative measures require more efforts in creating technical standards and ensuring that those standards are consistently applied, irrespective of any privacy incident.

Third, as platforms are growing exponentially with the rise of the digital economy, MOCI may not have sufficient capacity and resources to oversee the entire industry. To date, there are more than 4,000 ESOs registered at MOCI's ESO portal that includes both Indonesian and foreign companies (<https://pse.kominfo.go.id/>) and the number will continue to increase. It will take MOCI a substantial number of investigators and supervisors in order to carry out its mandate. Having a co-regulatory approach with a trusted partner will reduce the burden of MOCI resources, combining the need to seriously enforce personal data protection rules while maintaining a light-touch approach to internet regulations.

Fourth, as multiple regulators are active in the digital space, potentially applying their rules over the same activities, questions arise as to who has the authority to determine if a security measure by a firm with an equivalent level of protection standards with the PDP Bill has been met—should it be MOCI or sectoral supervisory authorities (e.g. OJK in the fintech sector, or Ministry of Trade in the e-commerce sector) that assume this role. For example, in electronic commerce (e-commerce, Articles 58 and 59 of GR 80/2019 mandate businesses to follow “common business practice” in managing personal data. This includes, among others, obtaining personal data legally, maintaining data accuracy and applying an acceptable protection system, and collecting only relevant data for limited and relevant purposes. For specific activities such as online marketing and advertising, article 17 of MOT Regulation No. 50/2020 emphasizes that personal data use must also follow “consumer protection principles and maintain healthy competition”.³ As article 55 of the draft PDP Bill reads that guidelines from business associations must “guarantee at least the equivalent level of protection standards with the bill”, the e-commerce industry association can play a role in creating technical e-commerce standards that harmonize the e-commerce rules and the personal data protection rules.

³ Government Regulation No. 80 of 2019 on Trading through Electronic Systems (GR 80/2019) and the Minister of Trade Regulation No. 50 of 2020 (MOT Regulation No.50/2020) on Provisions on Business Licensing, Advertising, Guidance and Supervision on Business Actors in Trading through Electronic Systems.

INDUSTRY ASSOCIATIONS AND CURRENT PRACTICES OF CO-REGULATORY ROLE

History of Co-regulation in Indonesia: Digital Economy & Financial Sector

Co-regulation bridges the state-control and self-regulation approach. It emphasizes the distribution of responsibilities between state and non-state stakeholders. State-controlled regulation is the traditional form of regulatory governance through the issuance of formal legislation and regulations enforced by state authorities. On the other hand, the rules under self-regulation of an industry are developed and enforced by the industry actors themselves. Bridging these two approaches, co-regulation combines both public and private regulatory monitoring and enforcement.

The room of interaction between formal regulatory authorities and the private industry bodies (either individually or collectively under business associations) remains to be developed. Co-regulation is more than a one-time intervention of seeking non-government stakeholders' input during policy creation. Rather, co-regulation is the result of continuous feedback, making it an experimental, mutual, and adaptive process (Finck, 2017; Torfing et al, 2016). The constant dialogue and adaptive environment differentiate co-regulation from other approaches. Implementation and policy enforcement are delegated in whole or in part by the government to the private sector based on mutually agreed upon standards and ongoing dialogue.

The type of delegation of regulatory authority from the government authorities to the private sector can vary depending on the sector. A private industry body may be part of a government panel that consults on policies. Such a body can also be granted authority to issue technical industry standards that are to be adopted as formal national rules. A more extensive form of co-regulation would allow a private body to issue regulations and policies over industry.

Co-regulation can be the most adequate option to address the regulatory challenges inherent to the digital economy. The existing government structure has been rife with regulatory fragmentation, outdated rules fashioned, and top-down legislative intervention that seems ill-suited. Therefore, as rules and standards stem from the industry themselves, co-regulation can be more relevant and responsive to the industry's needs.

However, both self-regulation and co-regulation have the risk of regulatory capture that is prone to anti-competitive behaviors. For example, if the private sector plays a role in stipulating technical standards or having a decision in the approval of business licensing of other companies (i.e. by virtue of industry recommendation as licensing requirement), a dominant private player may exert their influence to apply standards only to its own benefit, it may restrict access to other companies to fairly operate in the market.

The constant dialogue and adaptive environment differentiate co-regulation from other approaches. Implementation and policy enforcement are delegated in whole or in part by the government to the private sector based on mutually agreed upon standards and ongoing dialogue.

In Indonesia, a private body granted a certain regulatory role is known as a Self-Regulatory Organization (“SRO”). The first SRO was first introduced in the capital markets and securities sector in 1995 with the enactment of Law No.8 of 1995 on Capital Market. Since then, there has been an attempt to introduce a similar model in the digital sector, as will be discussed in the subsequent section of this paper.

SRO is given the authority to make regulations related to activities, which are binding, and must be followed by its members. There are three SROs in the Indonesian capital market structure, namely: Indonesia Stock Exchange (IDX), Indonesian Clearing and Guarantee Corporation (*Kliring Penjaminan Efek Indonesia* or KPEI), and Indonesian Central Securities Depository (*Kustodian Sentral Efek Indonesia* or KSEI). These three organizations are private limited liability companies (*Perseoran Terbatas* or PT) owned by securities companies. There is no state involvement in the shareholding structure of IDX, KPEI, or KSEI. The IDX, for example, has the authority to supervise securities companies and impose sanctions for prohibited market practices. The IDX also has a role in reviewing documents of companies that want to go public or issue securities in the stock exchange.

The concept of SRO has been introduced as a solution to govern digital finance, which similar to capital markets, has very dynamic market activities and therefore requires faster policy and supervisory responses. Since 2018, Indonesia’s Financial Services Authority better known as *Otoritas Jasa Keuangan* or OJK has been pushing for the creation of SROs to regulate the fintech sector. Fintech associations will be considered as the SROs serving as “the extension of OJK arm” and having the authority to impose sanctions over violations of their members. Chairman of OJK, Wimboh Santoso in 2020, made a remark about the importance of fintech associations as SROs to help OJK carry out the supervisory mandate because of the overwhelming consumer complaints that came to OJK every day (Setiawan, 2020).

The decision to allow fintech industry associations as “SROs” depicts a common practice within the heavily-regulated financial sector in Indonesia that empowers industry associations with certain authorities or mandates. Similar models can be found in other sectors such as insurance, financing, fintech lending, digital financial innovation, and payments. A common feature is the stipulation of an officially-endorsed association within the respective sectoral regulation followed by mandatory membership. Membership revocation will be the basis for revoking the entire business licenses, thus turning the associations into powerful organizations. Table 2 below provides examples of sectoral regulations that empower associations.

Table 2.
Sectoral Regulations that Empower Associations

No.	Sector	Legal Basis	Role of Associations
1	Fintech	P.OJK 77/ POJK.01/2016 (Peer to Peer Lending) and P.OJK 13/ POJK.01/2018 (Digital Financial Innovation)	Mandatory memberships for fintech lending companies and digital financial innovation firms in OJK-sanctioned associations.
2	Payment	BI Regulation 19/8/ PBI/2017 on National Payment Gateway	<p>Mandatory memberships for payment companies in BI-sanctioned associations (ASPI)</p> <p>The payment association (ASPI) is officially appointed as the technical standard-setting body. So far, ASPI has been championing the QR standard (QRIS) and the Open API payment standard (SNAP). Upon extensive discussions in ASPI working groups, final standards will be officially adopted by virtue of BI official decrees.</p>
3	Insurance and reinsurance	P.OJK 67 /POJK.05/2016 on Insurance Business License	<p>Mandatory memberships for insurance and reinsurance companies in OJK-sanctioned associations (Art. 70).</p> <p>Mandatory memberships in professional associations for expert officers, actuary officers, and internal auditors. Such professional associations will issue statements that the expert officers' candidates are not under sanction (Art. 55-60).</p> <p>Mandatory memberships in a professional association for insurance agents. Insurance agents receive an explicit mandate to perform agent registration on behalf of OJK. OJK has authority and access over the agent database maintained by Association (Art. 71).</p>
4	Insurance and re-insurance brokerage	P.OJK 68 /POJK.05/2016 on Business Licensing and Institutional Insurance Brokerage Companies, Reinsurance Brokerage Companies, and Insurance Loss Assessing Companies	<p>Mandatory memberships for insurance and reinsurance companies in OJK-sanctioned associations (Art. 45).</p> <p>Mandatory memberships in professional associations for insurance broker officers and expert officers. Such professional associations will issue statements that the expert officers' candidates are not under sanction (Art. 21-39)</p>
5	Financing Companies	P.OJK47 /POJK.05/2020, P.OJK on Business Licensing and Institutional Financing Companies and Sharia Financing Companies	<p>Mandatory memberships for financing companies in OJK-sanctioned associations (Art. 15 of P.OJK 47 / POJK.05/2020)</p> <p>Mandatory memberships in professional associations for finance officers, collection officers, and risk management officers. Such professional associations will issue statements that the expert officers' candidates are not under sanction (Art. 17 P.OJK 35 /POJK.05/2018)</p>
6	Securities brokers and underwriters	P.OJK 27/POJK.04/2014 on Licensing of Underwriter Representatives and Broker-Dealer Representatives	Mandatory memberships in professional associations for brokers and underwriters and participation in continuous professional education.

Source: Authors analysis

Industry Associations and Personal Data Protection: Growing Practices in Digital Finance

Sector-specific industry practices are important in defining personal data protection practices at more technical and detailed level. A key question to determine whether a sector-specific standard is necessary is whether the sector in question has distinct practices that deserve special treatment in personal data protection enforcement. For example, in other countries, easing collection of biometric information or automated data collection in Internet-of-Things may require stringent rules on the legitimate purpose of processing biometric information or for smart city purposes.⁴ Whereas in Indonesia, most cases arise within the digital finance sector. Financial service providers are developing a reliable Know Your Customer (KYC) system to minimize default risk by collecting personal data with high degree of personally identifiable information (PII). But this may also lead to a serious privacy impact in the case of data breach or data misuse.

This is mainly the reason why the Indonesian Fintech Association (AFTECH), the Indonesian Joint Funding Fintech Association (AFPI), and the Indonesian Payment Associations (ASPI), have been empowered by the regulators to actively co-regulate the fintech sector. Both AFPI and AFTECH have developed their own code of conduct, each with a dedicated section on managing personal data. These codes of conduct are constructed in accordance with various laws, government, and ministerial regulations on the principles of responsible data management, including cyber security and protection of user personal data as stated in Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions (GR No.71/2019), MOCI Regulation No. 20 of 2016 on Protection of Personal Data in Electronic Systems (MOCI Regulation No. 20/2016), Bank Indonesia Regulation 16/1/PBI/2014 on Consumer Protection for Payment System Services, and OJK Regulation (POJK) 13 of 2018 on Digital Financial Innovation in the Financial Services Sector. In addition, many fintech service providers have gone through audits and adopted international standards such as ISO 27001 in their data security measures.

As for AFPI, its power to co-regulate the fintech sector is further empowered by Article 48 of the OJK Regulation No. 77/POJK.01/2016 on Information Technology-Based Lending and Borrowing Services that mandates fintech providers to be a member of an association acknowledged by OJK. Through letter No. S5/D.05/2019 dated 17 January 2019, OJK appointed AFPI as the official association of information technology-based lending and borrowing services in Indonesia. As AFPI membership becomes mandatory for the financial services providers, AFPI has the power to develop self-regulatory instruments, monitor compliance and ensure enforcement towards their members.

⁴ See for example China's technical standard for facial recognition that restricts facial recognition only for identification purposes and not to make predictions about individuals (e.g., in relation to their health, work performance or interests). See <https://www.huntonprivacyblog.com/2021/04/29/china-publishes-draft-security-standard-on-facial-recognition/>

AFTECH Code of Ethics on Personal Data Protection

The role of industry associations in personal data protection in Indonesia's digital economy ecosystem is manifested by at least two major industry associations, namely AFTECH and AFPI. AFTECH argues that despite the stagnant progress of the PDP Bill deliberation, there are several related regulations in Indonesia and best practices that can be applied so that digital financial services in Indonesia can continue to develop responsibly (Interview 2, 2022). Thus, AFTECH developed and issued a Personal Data Protection Code of Ethics for its members to promote responsible digital financial innovation with its implementation (AFTECH, 2021). AFTECH's Code of Ethics is accessible to the public on their website and is discussed in more detail in Box 1 and Table 3 below.

Box 1. Getting to Know AFTECH

Established in 2016, the Indonesian Fintech Association (AFTECH) has become a forum for numerous fintech companies in Indonesia to discuss and collaborate with various stakeholders to encourage innovation technology and strengthen the competitiveness of the national fintech industry.

Three years after its founding, on 9 August 2019, AFTECH was officially appointed by the Financial Services Authority (Otoritas Jasa Keuangan or OJK) as the Association for Digital Financial Innovation Providers (Inovasi Keuangan Digital or IKD). This appointment has shown a co-regulatory approach in Indonesia's fintech ecosystem. Currently, AFTECH has more than 350 members consisting of start-up companies in the fintech sector, technology service providers and other financial services.

AFTECH has a vision to "Encourage Financial Inclusion through Digital Financial Services in Indonesia" and a mission to support the government's financial inclusion targets with four main pillars, namely: (i) Policy Advocacy; (ii) Community Collaboration; (iii) Literacy and Education; and (iv) Knowledge and Intelligence.

With its twelve working groups, AFTECH has participated in supporting the Indonesian parliament and the government—in particular the Ministry of Communication and Information—on providing insights into the Fintech industry as input in the development of the PDP Bill. Illegal practices that misuse personal data have become public and consumer complaints and the existence of legal certainty in relation to PDP will increase public confidence in fintech industry services.

Source: AFTECH (N.d.). <https://fintech.id/id/about#working-group> and Interview 2 (2022)

The Code of Ethics related to Personal Data Protection and Data Confidentiality in the Financial Technology Sector (Kode Etik terkait Perlindungan Data Pribadi dan Kerahasiaan Data di Sektor Teknologi Finansial) will be referred to as AFTECH Code of Ethics for PDP. The forming of this Code of Ethics was driven by its members' concerns on legal certainty to consumers as Personal Data Owners regarding the protection of personal data. In addition, it also intended to increase public confidence in using financial technology as well as to demonstrate AFTECH members' commitment to responsibility for the government and other financial service actors in conducting digital financial innovations.

Acknowledging the policymaking authority of the government, this AFTECH Code of Ethics for PDP was built upon two major regulations concerning PDP—MOCI Regulation No.20/2016 on Protection of Personal Data in Electronic Systems and Government Regulation No.71/2019 on the Implementation of Electronic Systems and Transactions. Table 3 showcase the key components of the Code of Ethics.

Table 3.
Components of AFTECH Code of Ethics for Personal Data Protection

Code of Ethics for Financial Technology Industry Regulation		
No.	Component	General Principles
1	Lawfulness, Fairness, and Transparency	Have a clear legal basis for processing Personal Data and comply with all applicable laws and regulations related to Personal Data.
		Using personal data in accordance with the purpose, appropriately, and not detrimental to the individual concerned.
2	Data Minimization	Only process Personal Data in accordance with the purposes that have been determined and approved by the Personal Data Owner.
3	Accuracy	Personal Data processed by AFTECH members must be kept accurate.
4	Integrity and Data Confidentiality	This PDP Code of Ethics does not specifically present the steps that need to be taken to safeguard Personal Data which is under the control of AFTECH members. However, this PDP Code of Ethics entrusts AFTECH members to take practical and responsible steps to protect Personal Data from the breach, loss, misuse, failure, or accidental alteration or destruction, in accordance with the provisions of the applicable laws and regulations.
5	Accountability	All Personal Data is processed responsibly and based on compliance with the provisions of the applicable laws and regulations. Control and processing of Personal Data is also carried out proportionally according to its purpose, and with a safe and accountable process.
6	Good Intention	The PDP Code of Ethics emphasizes that all Personal Data processing activities by AFTECH members are carried out in accordance with the approval obtained from the Personal Data Owner and in accordance with the provisions of the applicable laws and regulations, and AFTECH members have clarification and resolution mechanisms to address allegations and incidents of violations and /or failure to protect Personal Data.
		The PDP Code of Ethics does not regulate in detail the mechanism for clarification and resolution and entrusts all mechanisms, statements, and notifications regarding the violation of Personal Data owned by AFTECH members in accordance with the provisions of the applicable laws and regulations.

Sources: Process by the author from AFTECH. (2021). Kode Etik terkait Perlindungan Data Pribadi dan Kerahasiaan Data di Sektor Teknologi Finansial. <https://fintech.id/storage/files/shares/Kode%20Etik/Kode%20Etik%20AFTECH%20-%20Tf%20PDP.pdf>

AFPI Code of Conduct for the Responsible IT-based Lending and Borrowing Services

Another co-regulation effort was manifested through the establishment and implementation of the Joint Code of Conduct (CoC) between AFPI, AFTECH and AFSI (2019). Formed in 2019, the Joint-CoC on Responsible IT-based Lending and Borrowing Services (*Pedoman Perilaku Penyelenggara Teknologi Finansial di Sektor Jasa Keuangan yang Bertanggungjawab*) aims to serve as a guide for the associations' members consisting of hundreds fintech companies to run their business responsibly.

The Code of Conduct is mainly implemented based on three general principles: (i) Product Transparency and Product Service Offering Methods; (ii) Risk Management of New Products; and (iii) Application of the Principle of Good Faith.

Box 2. The Role of AFPI

The Indonesian Joint Funding Fintech Association (*Asosiasi Fintech Pendanaan Indonesia* or AFPI) was created to bridge Indonesia's Financial Services Authority (Otoritas Jasa Keuangan or OJK) and numerous peer-to-peer lending players in Indonesia. Similar to AFTECH which is involved in a co-regulatory approach, OJK was granted AFPI strategic role in carrying out regulatory and supervisory functions based on OJK Letter No. S-D.05/IKNB/2019 and OJK Regulation No.77 (POJK 77). That means peer-to-peer lending operators are required to register as AFPI members and abide by its Code of Conduct.

As a consequence, AFPI becomes the gatekeeper for overseeing its members. It can also declare if one of its members is violating the Code of Conduct before the government, in this case, is OJK, taking further investigation and reviewing the business license of that particular fintech company.

Sources: Suleiman (2021). Improving Consumer Protection for Low-Income Customers in P2P Lending. Center for Indonesian Policy Studies. <https://www.cips-indonesia.org/publications/improving-consumer-protection-for-low-income-customers-in-p2p-lending>

Enforcement of AFTECH Code of Ethics for Personal Data Protection and AFPI Joint Code of Conduct

On the enforcement process, AFTECH actively collaborates and coordinates with OJK, Bank Indonesia and all relevant stakeholders from both government and private sectors in improving the digital financial literacy of the Indonesian people and building a good fintech industry culture and digital financial services. This was done by prioritizing the principles of good governance, including through the implementation of a code of ethics for fintech operators (Interview 2, 2022).

AFTECH has an Honorary and Independent Ethical Council which is obliged and authorized to oversee the achievement of the implementation of the Code of Ethics by AFTECH members and has the right to receive, examine complaints, and impose sanctions on the association members who are deemed to have violated the association's Code of Ethics. The procedures and mechanisms of the examination process and the imposition of sanctions related to violations of the Code of Ethics are further regulated in the Bylaws and the Standard Operating Procedure (SOP) of the Honorary/Ethical Council.

In case the association member is proven to have violated the code of ethics or does not carry out their duties, the association will take further steps as follow:

1. The Honorary/Ethics Board accepts cases of violations of the Association's Code of Ethics originating from:
 - a) requests from regulators, namely OJK or BI;
 - b) a written complaint from a Member Association; and
 - c) AFTECH supervision of companies listed as Digital Financial Innovation companies at OJK.
2. The Honorary/Ethical Council may seek facts on alleged violations of the Code of Ethics accompanied by convincing evidence that there has been an alleged violation of the Association's Code of Ethics by AFTECH members.
3. The Honor/Ethics Council is required to summon in writing the AFTECH member suspected of violating the Code of Ethics within 14 working days after finding the facts of the alleged violation of the Code of Ethics, to examine and confirm whether or not there has been a violation of the Code of Ethics by AFTECH members, and to provide opportunities for the member concerned to provide explanations and defenses. The summons must be made no later than 7 (seven) working days before the date of the examination.

Based on the results of the examination, in the case the Honorary/Ethical Council finds that the member of the Association being examined is proven to have violated the Code of Ethics, the Honorary/Ethical Council has the right to impose sanctions in the form of:

- a) warnings;
- b) temporary suspension from AFTECH membership; or
- c) permanent termination of AFTECH membership.

Membership revocation can have serious consequence to the company. OJK regulation requires all registered companies to be member of the official association. Losing the membership means failing to comply with OJK requirements, which in turn can trigger OJK to revoke the company's business license. This means that AFTECH code of conduct has a stronger effect than a mere community authority, but it has direct impact on a member company's license to operate in the market.

Box 3. Case Study of RupiahPlus

AFTECH, which in 2019 transferred the SRO role for the online lending sector to AFPI, has also played a role in closing regulatory and supervisory gaps in the fintech lending sphere. The first high profile case involving data privacy and debt collection occurred in June 2018. RupiahPlus, then a payday lender registered at OJK, had an app that enabled the operator to access the borrower's contact list and use this access as leverage when the borrower failed to make repayment. RupiahPlus would contact individuals in the borrower's contact list and inform them about the borrower's failure to pay in an effort to discredit or embarrass the borrower (Sari, 2018). It came to light that this practice was not exclusive to RupiahPlus—almost all payday lenders, both registered and unregistered at OJK, used this practice. Borrowers consented to allow access to their contact list when they downloaded the app, but it was unclear whether it is legally necessary to obtain consent from each person listed in the contact book. It was also unclear if these calls constituted online “bullying” or harassment.

When this case emerged, OJK and AFTECH were not prepared to handle the situation. During July-September 2018 OJK and AFTECH conducted a series of hearings and consultations to investigate whether the action violated the law or the association's code of conduct. In a meeting led by OJK in early July 2018, RupiahPlus admitted their mistakes and promised to remedy the situation. OJK then asked AFTECH to expedite the process of establishing rules for responsible lending, which include the creation of details with respect to responsible privacy practices – which at that time had not existed. Also at that time, rules for investigating violations of members and independent committee to examine cases had not been established within AFTECH. At the request of OJK, AFTECH conducted informal inquiries into the practice of RupiahPlus, carried out by the relevant board members, and later by an assembled team of independent lawyers, in parallel with OJK's own investigation. Findings from AFTECH were used to complement OJK's findings, which led to sanction against the company. Eventually on the 26th of July 2018, OJK decided to impose suspension of licensing process for three months (Pitoko, 2018).

Only a few days before the sanction, on the 24th of July 2018, AFTECH eventually established a code of conduct for responsible lending that governed the more technical details of best practice lending, including data privacy and debt collection behavior. The Code had been prepared since April 2018 and had received written feedback from

OJK consumer protection department several times. Public pressure surrounding the Rupiahplus case also triggered OJK to give final clearance for AFTECH to issue the code of conduct. The code of conduct requires fintech companies / digital financial providers to maintain good faith in the collection, storage, and use of personal data of users or prospective users. Examples of use of personal data that are not in good faith include, among others:

1. Asking for personal data from prospective users without intending to provide services to such prospective users
2. Collecting personal data not relevant to the intended services
3. Collecting personal data outside of the data consented by the users
4. Collecting personal data without capacity to handle the personal data reliably

The code of conduct (further revised by AFTECH in 2019 and 2021, and AFPI in 2020⁵) served as a basis for the association to supervise its members, receive consumer complaints, and impose sanctions on non-compliant members. Sanctions can vary from formal warning to revocation of membership. When a company's membership is revoked, OJK can use this as the basis for revoking the platform's business license.

This case serves as an initial form of how industry association could play important role in the enforcement of privacy violations. AFTECH as industry body, in the absence of clear framework and at the request of OJK, complemented OJK investigation through "trial by peers" to determine whether the action of the company was considered common business norms or practices. The trial by peers were supported by the presence of independent lawyers who could give legal insights. In October 2018, AFTECH decided to formalize the rules to ensure the fairness and impartiality of the peer discipline process, while providing procedures for escalation to the independent committees.

⁵ The CoC updated by AFPI can be accessed here: <https://www.afpi.or.id/articles/detail/pedoman-perilaku-afpi#>

THE NEXT AVENUE: POTENTIAL CO-REGULATORY ROLE OF DATA PROTECTION OFFICER (DPO) ASSOCIATION

While there are already existing practices in the digital finance sector that can serve as a foundation to co-regulation in personal data protection, the upcoming PDP Bill creates ample opportunities for a DPO association to play a role in enforcing professional rules, ethical standards, and qualification or competence standards in personal data protection. This can potentially improve personal data protection standards by focusing rules and enforcement at the individual (i.e. a DPO within a company) and the board level to complement responsibilities and liabilities at corporate level.

Data Protection Officer (DPO) under Existing Regulations and the draft PDP Bill

Data Protection Officer (DPO) is an important part of the data protection ecosystem that MOCI is trying to build. This is acknowledged by MOCI's Strategic Plan 2020-2024 which includes the "development of the DPO ecosystem" as one of MOCI's priorities. It wants to create a regulatory framework where the DPO association can contribute optimally to the development of the DPO ecosystem (MOCI, 2021).

Although the term DPO in Indonesia is popularized by the draft PDP bill, attention to the importance of specialists in managing personal data in the digital space has been around longer. A "contact person" responsible to address concerns from data owners regarding the collection and management of their personal data was first introduced by Article 28 of MOCI Regulation No. 20 of 2016 on Personal Data Protection (MOCI Regulation No. 20/2016). This role is then extended by the PDP bill draft.

In the draft PDP bill, the roles and responsibilities of the DPO are closely related to the legal responsibilities of personal data processors and personal data controllers.⁶ Both data controllers and processors are liable to handle personal data with respect to individual privacy and the rights of data owners. Responsible, transparent, and limited use and processing of personal data are therefore mandated to processors and controllers. DPO helps data controllers and processors to perform these roles in compliance with applicable data protection rules.

However, not all controllers and processors are required to appoint a DPO. The PDP bill adopts a risk-based approach like that of the European Union General Data Protection Regulation (GDPR)—it encourages processors and controllers to apply protective measures corresponding to the risk level of their data handling activities. As such, the appointment of a DPO is only mandated for processors and controllers that engage in the following activities:

⁶ Pursuant to the general framework, a data controller exercises ultimate control over the purposes for which and the means by which personal data is processed, while data processor is typically a third-party that processes personal data only on behalf of the controller.

- a. Processing of personal data for public services;
- b. Large-scale regular and systematic monitoring of personal data; and
- c. Large-scale processing of specific personal data and/or personal data related to criminal acts.

The PDP draft bill uses the term “officials or officers carrying out personal data protection functions” (*Pejabat atau Petugas Pelindung Data Pribadi* or PPPDP) to refer to a DPO. The word “officials” signs that public institutions that process and control personal data are also mandated to assign a DPO to help them comply with their institutional obligations.

According to article 46 of the PDP bill, the roles of DPO include:

- a. Inform and provide advice to the Personal Data Controller or Personal Data Processor in order to comply with the provisions of this Law;
- b. Monitor and ensure compliance with this Law and the policies of the Personal Data Controller or Personal Data Processor, including assignments, responsibilities, awareness-raising and training of parties involved in the processing of Personal Data, and related audits;
- c. Provide advice on assessing the impact of protecting Personal Data and monitoring the performance of Personal Data Controllers and Personal Data Processors; and
- d. Coordinate and act as a liaison for issues related to the processing of Personal Data, including conducting consultations on risk mitigation and/or other matters.

DPO Roles and Accountability

As per the latest publicly accessible PDP bill draft, details on the DPO accountability, sanctions, and responsibilities in each step of the data cycle are currently missing. One interpretation of the missing sanctions and accountability from the bill is that similar to GDPR, as the DPO will only perform a consulting role for the controllers and processors and sanctions over failures to meet the protection standards will be imposed to the controllers and processors, and not the DPO (Box 1). This will arguably affect the role of DPO associations with regards to the development of code of conducts for DPO professionals, which will be explained in the next chapter.

There is, however, a noticeable different choice of words between the PDP bill and the GDPR when it comes to DPO. Article 38 of the GDPR reads that the DPO shall “ensure” while article 45 of the PDP bill states that PPPDP “implements” the data protection functions. According to MOCI (2021) this means that instead of acting only as a consultant, PPPDP must implement all functions of personal data protection which include legal compliance, governance, management, and technical functions. Nonetheless, details on DPO’s roles and responsibilities are expected to be covered by implementing regulations of the PDP.

DPO training and certification

Although article 45 of the PDP bill draft states that DPO must be appointed on the basis of professional qualities, knowledge of the law and practice of personal data protection, and ability to fulfill their duties, a mechanism through which individuals can meet such qualities is yet to be covered by the latest PDP draft, nor it is by other prevailing laws and regulations in Indonesia. MOCI's Strategic Plan 2020-2024 suggests that implementing rules and regulations on DPO standardization will follow suit after the PDP bill passes the house.

Professionalism referred to by Article 45 of the PDP bill has an idealistic dimension and an institutional dimension (Simon, 2003). The idealistic dimension sees DPO as a professional that voluntarily commits to both the client's interest as well as the public values. The institutional dimension explores ways to govern and support these ideal expectations to the DPO, including roles for professional associations to self-regulate ethical conduct and develop mechanisms to maintain the professional quality of the members.

Self-regulation by associations is typically manifested in codes of practice, industry-based accreditation systems, and voluntary adoption of technical standards (Hepburn, 2009). However, as the draft bill gives little clarification on which among these options would be adopted to support the quality of the DPO, it remains a discussion on how far can DPO associations take part in co-regulating the profession.

Different models of professional certifications

Nonetheless, laws and regulations in Indonesia have attempted to involve associations to ensure a certain level of professionalism for some lines of work. Law No. 18 of 2003 on Advocates, for example, set minimum requirements for individuals to be qualified as a lawyer and perform their roles in and outside of courts. To become an advocate, individuals must go through the required educational stages—they must have a Bachelor's degree obtained from law faculties, Sharia faculties, military law colleges and police academies⁷, after which they must complete the legal professional course known as the Special Education for Advocates (*Pendidikan Khusus Profesi Advokat* or PKPA), and pass the bar exam. The PKPA is run by an advocates association (similar to a bar association), showing a shared responsibility between the government and non-state actors (i.e. associations) in maintaining professionalism in the profession.

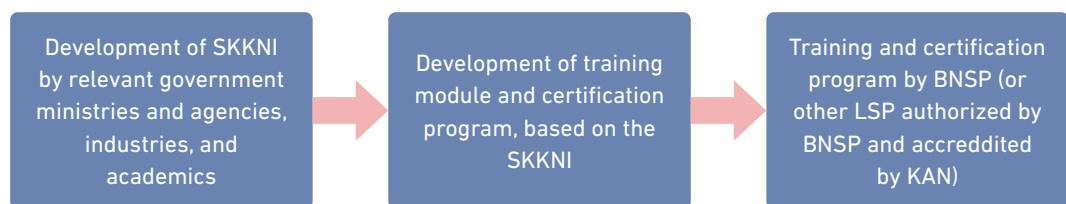
Other professions are governed differently through the National Job Training System (*Sistem Pelatihan Kerja Nasional* or SPKN) as regulated by Law No. 13 of 2003 on Manpower (Labor Law) jo. Government Regulation No. 31 of 2006 on National Job Training System (GR 31/2006). SPKN is a professional training and competency certification mechanism by the National Professional Certification Agency (*Badan Nasional Sertifikasi Profesi* or BNSP) or other Professional Certification Agency (*Lembaga Sertifikasi Profesi* or LSP) authorized by BNSP. This scheme has covered professional certifications in various sectors, including health services and social activities, information and communication, construction, water supply, and waste management.

⁷ Article 2 (1) of Advocate Law

The training and certification mechanism must follow the Indonesian National Work Competency Standard (*Standar Kompetensi Kerja Nasional Indonesia* or SKKNI) which covers minimum requirements of knowledge, skills, and/or expertise as well as work attitudes that are relevant to the implementation of the assigned duties and job requirements. *Lembaga Sertifikasi Profesi* that wishes to run training and certification programs based on the *Standar Kompetensi Kerja Nasional Indonesia* can apply for accreditation by the National Accreditation Committee (*Komite Akreditasi Nasional* or KAN) by referring to the procedure in Law No. 20 of 2014 on Standardization and Conformity Assessment.

In the ICT sector, the MOCI Regulation No. 24 of 2015 on the Enforcement of the *Standar Kompetensi Kerja Nasional Indonesia* in the Information Communication Sector (MOCI Regulation No. 24/2015) has set some ground rules that, among others, mandate both private and public institutions in the ICT sector to have their workers certified under the SKKNI.⁸ There are 52 *Standar Kompetensi Kerja Nasional Indonesia* developed by the MOCI under the National Job Training System scheme (MOCI, 2021). Therefore, it is possible to have the DPO standards, competencies, and certifications developed as a sub-sector under this framework.

Figure 4.
Training and competency certification mechanism under the SPKN



Sources: Authors' analysis

Under this scheme, the DPO associations can take part in the development of SKKNI in the sub-sector of data protection. Associations can also apply to *Badan Nasional Sertifikasi Profesi* and *Komite Akreditasi Nasional* to be authorized as *Lembaga Sertifikasi Profesi* to run the certification and training program for DPO. MOCI's Directorate of Informatics and Governance of Applications will also be involved in each of the processes. In order to ensure that this will not become a burden for newly-formed tech startups, a tiering requirement may be applied to require only certain companies to comply, for example based on the company size, or the amount of data processed.

According to MOCI (2021, p.151), the *Standar Kompetensi Kerja Nasional Indonesia* will be designed based on the ASEAN Qualification on Reference Framework (AQRF) with the standard format of the ILO (International Labor Organization) to comply with recognized global standards.

⁸ According to article 6 of MOCI Regulation 24/2015, this is conditional upon the availability of at least two LSPs in each sub sector of the SKKNI.

Although the PDP bill gives minimal indication on whether DPOs are required to be certified, and if it is, what kind of certification mechanism would be applied and which government and non-government stakeholders would be involved, the Indonesian Association of Data Privacy Professionals (*Asosiasi Profesional Privasi Data Indonesia*) has started to run a training program and issue DPO certificates upon completion of the program. It also offers a paid membership, along with the perks of data protection events and resources for the members. As there has yet to be regulatory backing on the certification program, enrollment and participation in the program should not affect one's legality to perform roles as a DPO. It may, however, be useful for individual professional development and gives an additional selling point as a data protection professional.

Association Membership and Ethical Role

Another way where DPO associations can take part in the data protection ecosystem is by the formulation of codes of professional conduct to ensure that the DPO is maintaining a high level of professionalism in performing their roles. Some areas that can be covered in the codes include DPO responsibility to their clients and employers, commitment to legal compliance and public interest, impartiality, and effort to self-improvement—all of which are relatively unelaborated in the PDP bill.

However, if association membership and formal certification are not mandated by the legislation, enforcement of the codes as well as members' incentive to comply with the codes may remain sub-optimal. Contrary to Law No. 18/2003 where advocates are obliged to comply with the code of ethics developed by the advocates' organization under the risk disbarment for noncompliance, a similar provision for DPO in the PDP bill is non-existent. For the time being, neither the Indonesian Association of Data Protection Practitioners nor the Indonesian Association of Data Privacy Professionals—two of the most active DPO associations in Indonesia—have developed a code of ethics for their members.

Box 4. **The Indonesian Association of Data Protection Practitioners**

*DPO association as a communication platform for data protection practitioners
in Indonesia*

The Indonesian Association of Data Protection Practitioners (*Asosiasi Praktisi Perlindungan Data Indonesia*) is one of the DPO associations in Indonesia registered in the Ministry of Law and Human Rights. Its first and foremost goal is to provide a communication platform for DPO professionals as well as to be a liaison between stakeholders regarding the development of data protection policies in Indonesia. It offers free membership for data practitioners across different digital sectors.

So far, it has organized several data protection seminars and trainings in relation to both generic and industry-specific themes. Topics are adjusted according to the needs of the

members as well as other relevant topics that can help increase understanding and awareness of responsible digital data activities in compliance with Indonesian laws and regulations. It brings industry experts to speak to members on a wide range of privacy-related subjects.

Regarding the self-regulatory authority of the association to develop ethical codes for the members, the association representatives highlight that they will wait for the development of the PDP bill and see if ethical conduct for members will fit into the DPO ecosystem that MOCI is trying to build.

The same attitude is also expressed in relation to DPO certification by association. In contrast to the Indonesian Association of Data Privacy Professionals which has started to run training and certification programs, the Indonesian Association of Data Protection Practitioners chooses to wait if such a mechanism will be supported by the PDP law.

The diverse background in the privacy profession also poses a challenge to develop codes of conduct.

The diverse background in the privacy profession also poses a challenge to develop codes of conduct. Privacy professions are filled with technologists, engineers, and lawyers, each with a different perspective on work around data protection regulations. Further, as the PDP Bill positions DPO as a consultant for data controllers and processors, there is the issue of DPO accountability—to what extent a DPO is responsible for data violation by controllers or processors, and how can the code of conduct reflect this accountability.

In the case of data breaches, with the existing regulatory framework in Indonesia for personal data protection, APPDI views that the responsibilities are embedded to the management team and not DPO (Interview 1, 2022). That is because the DPO plays a role as the advisor to the management team of particular company or institution which in this case is the data controller. In the end, the management team has the freedom to decide whether DPO's advice will be taken or not responding to the case. Hence, the main responsibility of a DPO is to advise and ensure that data controllers adhere to the law.

Comparison with GDPR

Similar to the PDP bill, the role of DPO in the GDPR is closely related to the controllers' and processors' liability to comply with certain standards and requirements in their data activities. Article 37 of the GDPR mandates processors and controllers to appoint a DPO in activities such as large-scale processing of special categories of personal data, regular and systematic monitoring of data subjects on a large scale, and data processing by a public authority.

Further, article 39 of the GDPR stresses that DPO shall be appointed on the basis of "professional qualities", and particularly "expert knowledge of data protection law and practices" to fulfil their task as mentioned in Article 39 of GDPR.

Beyond provisions in the GDPR, the EU also issued Guidelines⁹ on Data Protection Officers (2017) where controllers and processors of personal data are encouraged to consider the following qualifications in appointing a DPO:

- expertise in national and European data protection laws and practices including an in-depth understanding of the GDPR;
- understanding of the processing operations carried out;
- understanding of information technologies and data security;
- knowledge of the business sector and the organization; and
- ability to promote a data protection culture within the organization

As article 39 (2) of the GDPR emphasizes that the DPO must take into account different levels of risk associated with different nature, scope, context and purpose of the processing operations, the necessary level of expert knowledge should be determined according to the data processing operations carried out and the protection required for the personal data being processed. For example, complex data processing activity, or where a large amount of sensitive data is involved, may require a DPO with a higher level of expertise (EU, 2017).

However, the GDPR does not mandate any certification or formal qualification for individuals to be a DPO. In practice, privacy organizations such as the International Association of Privacy Professionals (IAPP) has engaged in various support activities for a DPO, including offering courses and certifications relevant to the DPO roles and responsibilities such as Certified Information Privacy Professional (CIPP), Certified Information Privacy Manager (CIPM), and Certified Information Privacy Technologist (CIPT). These credentials are accredited by the American National Standards Institute (ANSI) under the International Organization for Standardization (ISO) standard 17024: 2012—ensuring that they are recognized globally.

In France, a few extra steps are taken by the Commission nationale de l'informatique et des libertés (CNIL)—the country's Data Protection Authority—to facilitate DPO certifications. Since 2018, the CNIL has approved third-party organizations that issue a DPO skills certification, and keeps a list of such organizations (CNIL, n.d.). The certification is only accessible after 2 years of professional experience in data protection, or 2 years in any field and at least 35 hours' training on the subject (CNIL, n.d.). It is valid for 3 years.

⁹ The guideline is accessible here <https://ec.europa.eu/newsroom/article29/items/612048>

The certification, albeit not mandatory in order to be a designated DPO, helps both DPO candidates and organizations to comply with the GDPR. For the former, the certification constitutes a proof of their adequacy with the level of knowledge requirement imposed by Article 39 of the GDPR. For the latter, certifications help designate qualified individuals as the DPO.

DPO in Spain: Central Roles of the Data Protection Agency

Among other EU member states subject to the GDPR regime, Spain takes a few extra steps further in governing the DPO—by developing a certification scheme under the supervision of the Spanish Data Protection Agency (*Agencia Española de Protección de Datos* or AEPD). Together with the National Entity of Accreditation (*Entidad Nacional de Acreditación* or ENAC), AEPD is developing a DPO certification scheme with standards equivalent to that of the ISO 17024 (IAPP, 2017).

The certification program can be performed by entities that meet the criteria and requirements established by the Certification Scheme of Data Protection Officers from the Spanish Data Protection Agency (DPO-AEPD Scheme) (2017). As it is based on technical competence and capacity to certify, the body must obtain and maintain accreditation by ENAC to certify individuals to be a DPO in compliance with the DPO-AEPD Scheme. AEPD regularly updates the list of accredited certification bodies and regularly verifies the certification body for compliance with the required obligations.

According to section 6.3. of the DPO-AEPD Scheme, prior to sitting on the certification exam, DPO candidates must meet one of the following prerequisites:

1. Demonstrate professional experience of at least five years on projects and/or activities and tasks related to DPO functions regarding data protection;
2. Demonstrate professional experience of at least three years on projects and/or activities and tasks related to DPO functions regarding data protection, and at least 60 hours of recognized training on subjects related to the programme;
3. Demonstrate professional experience of at least two years on projects and/or activities and tasks related to DPO functions regarding data protection, and at least 100 hours of recognized training on subjects related to the programme;
4. Demonstrate at least 180 hours of recognized training on subjects related to the programme.

Other than detailing professional qualifications for DPO, the AEPD also developed a code of ethics that DPO candidates must agree on prior to taking on the certification program.¹⁰ Failure to comply with the principles, values, and criteria in the code may result in the suspension or removal of the certification.

¹⁰ Section 6.4. jo. Annex III of the DPO-AEPD Schemes

CONCLUSIONS AND RECOMMENDATIONS

The Ministry of Communications and Informatics has been developing various measures to ensure adherence to personal data protection best practices. These include enforcement mechanisms covered in GR 71. However, as digital transactions are growing exponentially, there are urgent needs to complement these measures with professional and technical sector-specific standards, preventative measures, and engage non-state actors in enforcement mechanisms. Unique to Indonesia, especially in financial services, industry associations have been playing this role as “self-regulatory-organizations” that complement the supervision of regulated entities.

Recently there has been precedent to expand this into digital finance, including in the event of violation of personal data protection. The RupiahPlus case in 2018 led to the creation of an industry code of conduct for responsible digital finance, which includes personal data protection best practices, and later perfected with industry code of conduct on personal data protection. All of these were initiated by industry associations, with full endorsement by the financial regulator, OJK. This model can be adopted for digital platforms in general, taking the opportunity of the upcoming PDP bill, which enables a similar structure to the co-regulatory approach.

Meanwhile, although the DPO organizations are still in their infancy, practices in other jurisdictions show that they can serve as potential co-regulatory partners to uphold adherence to personal data protection standards.

From Table 4 below, CIPS identified seven associations in Indonesia’s digital economy system that work in data protection and data protection officers. The extensive list of information technology associations and communities are provided by MOCI under the Directorate General of Application Informatics (MOCI, 2019). With the rapid development in this sector, the list of business and professional associations may grow further beyond the coverage of this paper.

Table 4.
List of Associations Related to the Digital Economy Ecosystem and Data Protection Officer in Indonesia

No.	Institution Name	Acronym	Type of Association	Year Founded
1	Asosiasi Fintech Indonesia (Indonesia Fintech Association)	AFTECH	Industry	2016
2	Asosiasi Fintech Pendanaan Indonesia (The Indonesian Joint Funding Fintech Association)	AFPI	Industry	2019
3	Asosiasi Fintech Syariah Indonesia (The Indonesian Sharia Fintech Association)	AFSI	Industry	2018
4	Asosiasi E-commerce Indonesia (Indonesian E-commerce Association)	idEA	Industry	2012
5	Asosiasi Sistem Pembayaran Indonesia (Indonesia Payment System Association)	ASPI	Industry	2011
6	Asosiasi Praktisi Pelindungan Data Indonesia (Indonesian Association of Data Protection Practitioners)	APPDI	Professional	2020
7	Asosiasi Profesional Privasi Data Indonesia (Indonesian Association of Data Privacy Professionals)	APPDI	Professional	2020

Sources: Author analysis and compilation

Leveraging the existing practices of these organizations (and any other new organization in the future), our recommendations for future improvement are as follows:

- Allow and enable industry associations their own flexibility to develop their own sector-specific technical standards. These may include very technical matters such as data collection and processing in biometric, digital finance, smart city / Internet of Things, and many others.
- Regulatory oversight is needed to ensure that these industry associations and standards are properly supervised and audited by the regulatory authority. In the case of PDP, the authority will be the one designated by the PDP Bill.¹¹ This is aimed to foster democratic decision making at the associations, setup checks and balances, and prevent the associations from “capture” by dominant players from anti-competitive behaviors such as setting up barrier to entry for new players. The interaction between the regulator and the association serves as the foundation for the co-regulation.
- Engage regular regulatory consultation for any industry self-regulatory making, such as the development of code of conducts. The financial regulators have been doing this, as evidenced by intense communication at the development of responsible lending code of conduct or payment standards that occurred throughout the process of standard-making. These create dynamic balance between regulatory and commercial interests.

¹¹ The supervisory and regulatory authority over personal data is one of the most debated topics in the PDP Bill. While the Executive Government prefers MOCI as the regulator, the parliament insisted on creating a new independent agency. As of June 2022, the draft would likely defer the issue to the President.

-
- Focus the development of technical standards at professional level, in this case DPO as profession. The European experience demonstrates that although there is no mandatory DPO requirement, the level of high-quality technical details of DPOs issued by the EU or national data protection agencies has encouraged the industry to adopt to these standards. In turn, the Government can officially endorse one or several DPO associations to be the official professional standard setting bodies in the country.
 - At the regulatory level, foster regulatory collaboration among data authorities (MOCI or any entity further appointed in the Bill) and sectoral regulators (OJK, BI, the Ministry of Health, etc.) to establish certain benchmarks so that any industry standards would comply with both PDP regulation and their sector-specific regulations.

REFERENCES

- AEPD [Agencia Española de Protección de Datos]. (2017). *Certification Scheme of Data Protection Officers from the Spanish Data Protection Agency (DPO-AEPD Scheme)*. AEPD. Retrieved from <https://www.aepd.es/sites/default/files/2019-12/scheme-aepd-dpd.pdf>
- AFPI. (2019). *Pedoman Perilaku Pemberian Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi Secara Bertanggung Jawab*. Retrieved from <https://www.afpi.or.id/articles/detail/pedoman-perilaku-afpi#>
- AFTECH, AFPI, and AFSI. (2019). *Pedoman Perilaku Penyelenggara Teknologi Finansial di Sektor Jasa Keuangan yang Bertanggungjawab*. Retrieved from [https://fintech.id/storage/files/shares/Kode%20Etik/Joint%20CoC%20-%20AFTECH%20AFSI%20AFPI%20\[PUBLIC\].pdf](https://fintech.id/storage/files/shares/Kode%20Etik/Joint%20CoC%20-%20AFTECH%20AFSI%20AFPI%20[PUBLIC].pdf)
- AFTECH. (2021). *Kode Etik terkait Perlindungan Data Pribadi dan Kerahasiaan Data di Sektor Teknologi Finansial*. Retrieved from <https://fintech.id/storage/files/shares/Kode%20Etik/Kode%20Etik%20AFTECH%20-%20TF%20PDP.pdf>
- AFTECH. (n.d.). *Tentang Kami*. Retrieved from <https://fintech.id/id/about#working-group>
- Aprilianti, I & Dina, SA. (2021). *Co-regulating the Indonesian Digital Economy*. Center for Indonesian Policy Studies. Retrieved from <https://www.cips-indonesia.org/publications/co-regulating-the-indonesian-digital-economy>
- Audrine, P & Murwani, A. (2021). *Implementing the Digital Economy Enabling Environment Guide: A Case Study from Indonesia*. Center for Indonesian Policy Studies. Retrieved from <https://www.cips-indonesia.org/publications/implementing-the-digital-economy-enabling-environment-guide%3A-a-case-study-from-indonesia>
- CNIL [Commission nationale de l'informatique et des libertés]. (n.d.). *Practical Guide for Data Protection Officers*. Retrieved from https://www.cnil.fr/sites/default/files/atoms/files/cnil-gdpr_practical_guide_data-protection-officers.pdf
- Devi, Z.M. (2015). *idEA Bakal Terbitkan Kode Etik Khusus e-Commerce*. Marketeers. Retrieved from <https://www.marketeers.com/idea-bakal-terbitkan-kode-etik-khusus-e-commerce?amp=1>
- EU. (2017). *Guidelines on Data Protection Officers (DPOs)*. European Union. Retrieved from <https://ec.europa.eu/newsroom/article29/items/612048>
- Finck, M. (2017). *Digital Regulation: Designing a Supranational Legal Framework for the Platforms Economy*. LSE Law, Society and Economy Working Papers, 15/2017.
- Google, Temasek, & Bain & Company. (2021). *e-Conomy SEA 2021 Roaring 20s: The SEA Digital Decade*. https://www.bain.com/globalassets/noindex/2021/e_conomy_sea_2021_report.pdf
- Hepburn, G. (2018). *OECD Report: Alternatives to Traditional Regulation*.
- Hepburn, G., (2009). *Alternatives to traditional regulation. Report prepared for the OECD Regulatory Policy Division*. <https://www.oecd.org/gov/regulatory-policy/42245468.pdf>
- IAPP. (2017). *Here's what it takes to be a certified DPO in Spain*. IAPP. Retrieved from <https://iapp.org/news/a/heres-what-it-takes-to-be-a-certified-dpo-in-spain/#:~:text=Certification%20bodies'%20evaluators%20will%20need,years'%20experience%20in%20either%20data>
- Karunian. (2020). *Kawal Pembahasan RUU Pelindungan Data Pribadi, Koalisi Advokasi RUU PDP serahkan usulan DIM Alternatif kepada DPR RI*. Retrieved from: <https://elsam.or.id/kawal-pembahasan-ruu-pelindungan-data-pribadi-koalisi-advokasi-ruupdp-serahkan-usulan-dim-alternatif>
- MOCI [Ministry of Communication and Informatics]. (2019). *Komunitas TIK*. Retrieved from <https://aptika.kominfo.go.id/category/data-aptika/komunitas/>
- MOCI [Ministry of Communication and Informatics]. (2021). *Grand Design Pembentukan Data Protection Officer (DPO) Indonesia*, Directorate General of Information Technology Applications MOCI.

Pitoko, R.A. (2018). Dapat Sanksi, RupiahPlus Dilarang Ajukan Izin ke OJK selama Tiga Bulan. Kompas. Retrieved from <https://ekonomi.kompas.com/read/2018/07/26/192744126/dapat-sanksi-rupiahplus-dilarang-ajukan-izin-ke-ojk-selama-tiga-bulan?page=all>.

Riyadi, G. (2021). Data Privacy in the Indonesian Personal Data Protection Legislation. Center for Indonesian Policy Studies. <https://www.cips-indonesia.org/publications/data-privacy-in-the-indonesian-personal-data-protection-legislation>

Sari, F. (2018). *OJK akan jatuhkan sanksi kepada fintech RupiahPlus*. Kontan. Retrieved from <https://keuangan.kontan.co.id/news/ojk-akan-jatuhkan-sanksi-fintech-rupiah-plus>

Setiawan, K. (2020). *Bos OJK Hampir Setiap Hari Terima Surat Komplain Soal Fintech*. Tempo Bisnis 18 November 2020. Retrieved from <https://bisnis.tempo.co/read/1406552/bos-ojk-hampir-setiap-hari-terima-surat-komplain-soal-fintech/full&view=ok>

Simon, William. (2003). 'Who Needs the Bar?: Professionalism Without Monopoly', Florida State University Law Review, Vol. 30 (4), pp.639-658

Suleiman, A. (2021). *Improving Consumer Protection for Low-Income Customers in P2P Lending*. Center for Indonesian Policy Studies. <https://www.cips-indonesia.org/publications/improving-consumer-protection-for-low-income-customers-in-p2p-lending>

Sutanto, T. (n.d.). *Asosiasi Sistem Informasi Indonesia*. Retrieved from http://aisindo.org/wp-content/uploads/2014/07/SistemInformasi_sebagai_PROFESI.pdf

Torring, J., Sørensen, E., & Røiseland, A. (2019). *Transforming the public sector into an arena for co-creation: Barriers, drivers, benefits, and ways forward*. Administration & Society, 51(5), 795-825.

Interviews

Interview 1: A Chairman & a Deputy of the Association of Indonesian Data Protection Practitioners (2022, April). Personal communication.

Interview 2: A Deputy Secretary-General & Head of The Personal Data Protection Task Force at Indonesian Fintech Association (2022, April). Personal communication.

ABOUT THE AUTHOR

Ajisatria Suleiman is a regulatory affairs practitioner specializing in the digital economy and digital finance. He has assisted regional and national internet as well as digital finance industry associations, international development agencies, global tech companies, and local startups. His research interests cover personal data protection, digital sovereignty, and digital finance. He is trained as a lawyer with a bachelor's degree from the University of Indonesia, and a master's degree from Erasmus University of Rotterdam and University of Hamburg.

Pingkan Audrine is a Researcher at Center for Indonesian Policy Studies, focusing on the topic of Economic Opportunities. She obtained her bachelor degree in Political Science from Parahyangan Catholic University. Prior to joining CIPS, Pingkan had experiences working in national broadcasting radio, international office at higher education institution and Office of the UN Resident Coordinator in Indonesia, and organizing multi-stakeholder events.

Thomas Dewaranu is a Researcher at CIPS. He holds a master's degree in public policy from the Australian National University and a bachelor's degree in law from Universitas Indonesia. His research interests cover rural development and poverty reduction. Prior to joining CIPS, he worked in a commercial law firm in Jakarta, providing legal services to local and multinational companies.

JOIN OUR SUPPORTERS CIRCLES

Through our Supporters Circles, you, alongside hundreds of others, enable us to conduct our policy research and advocacy work to bring greater prosperity to millions in Indonesia.

Those in our Supporters Circles get the opportunity to engage in the work of CIPS on a deeper level. Supporters enjoy:

- Invitation to CIPS' annual Gala Dinner
- Exclusive Supporters-only briefings by CIPS leadership
- Priority booking at CIPS-hosted events
- Personal (Monthly/Quarterly) Supporters-only update emails and videos
- Free hard copy of any CIPS publication upon request



For more info, please contact anthea.haryoko@cips-indonesia.org.

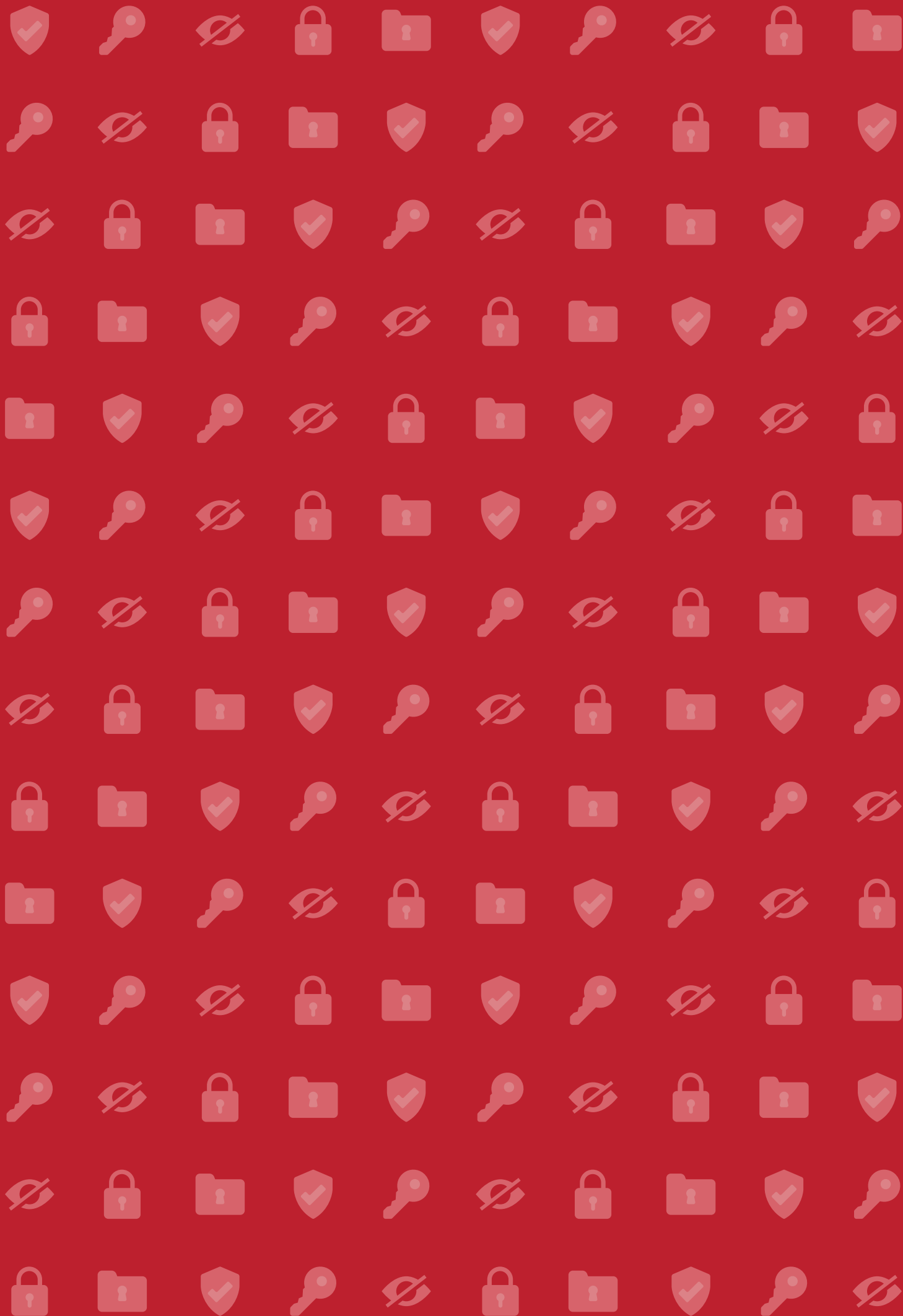


Scan to join









ABOUT THE CENTER FOR INDONESIAN POLICY STUDIES

Center for Indonesian Policy Studies (CIPS) is a strictly non-partisan and non-profit think tank providing policy analysis and practical policy recommendations to decision-makers within Indonesia's legislative and executive branches of government.

CIPS promotes social and economic reforms that are based on the belief that only civil, political, and economic freedom allows Indonesia to prosper. We are financially supported by donors and philanthropists who appreciate the independence of our analysis.

KEY FOCUS AREAS:

Food Security & Agriculture: To enable low-income Indonesian consumers to access more affordable and quality staple food items, CIPS advocates for policies that break down the barriers for the private sector to openly operate in the food and agriculture sector.

Education Policy: The future of Indonesia's human capital need to be prepared with skills and knowledge relevant to the 21st century. CIPS advocates for policies that drive a climate of healthy competition amongst education providers. Such competition will drive providers to constantly strive to innovate and improve education quality for the children and parents they serve. In particular, CIPS focuses on the improvement of operational and financial sustainability of low-cost private schools who serve the poor.


Economic Opportunities: CIPS believes that strong communities provide a nurturing environment for individuals and their families. They must have the rights and capacities to own and manage their local resources and to ensure healthy and sound living conditions for the development and prosperity of the community.


www.cips-indonesia.org

 facebook.com/cips.indonesia

 [@cips_id](https://twitter.com/cips_id)

 [@cips_id](https://www.instagram.com/cips_id)

 [Center for Indonesian Policy Studies](#)

 [Center for Indonesian Policy Studies](#)

Jalan Terogong Raya No. 6B
Cilandak, Jakarta Selatan 12430
Indonesia