International Journal of Social Science and Human Research

**ISSN (print): 2644-0679, ISSN (online): 2644-0695**

Volume 07 Issue 08 August 2024

DOI: 10.47191/ijsshr/v7-i08-41, Impact factor- 7.876

Page No: 6153-6158

# The Readiness for Privacy Compliance in Indonesia Before October 2024

**Adith Aulia Rahman[1], Awaludin Marwan[2], Andi Tri Haryono[3]**

[1]Primagraha University

[2]Faculty of Law, Bhayangkara University

[3]Faculty of Economics and Business, Wahid Hasyim University

**ABSTRACT**: Privacy law in Indonesia is stipulated in Law No. 27 of 2022 will be fully effective on 17th October 2024. The duration of 2 years adjustment will be ended and many institutions and companies are preparing for compliance. The PDP Law was prepared to empower data privacy by applying to all companies that process the personal data of Indonesian citizens. This law refers to European privacy law: GDPR. Currently, the Indonesian government is preparing a Government Regulation as a derivative regulation of the PDP Law. In this article, the author will explain the most important parts and topics regarding this regulation as well as an assessment of its actual results and impact. Many government institutions are not ready to comply with this PDP Law. On the other hand, the financial industries, like banking as well as e-commerce, are already preparing a good privacy governance in facing fully applied PDP Law before October 2024.

**KEYWORD:** PDP, Privacy, Subject Data, Data Processing

## INTRODUCTION

In the digital era, privacy data is not only 'new oil,' but also 'gold.'[1] Privacy data can be exploited for business, political, and bad purposes.[2] Cybercrime and exploiting privacy data can be a huge challenge of innovation.[3] There are conceptual frameworks to provide adequate protection among the people and at the same time supporting digital transformation.[4] The principles of data privacy protection is a key fundamental component to inspire digital modernization. [5]

Several studies present comprehensive data, a study conducted by the OECD shows that the GenAI transformation of the digital ecosystem is projected to expand its market to USD 207 billion by 2030 (OECD Digital Economy Outlook 2024)[6]. In addition, another report shows that IoT development has exceeded the market capitalization of $100 billion for the first time in 2017, and is expected to increase to $1.6 trillion by 2025 (UN Digital Economy Report 2024)[7]. According to OECD projections, by 2026, 70% of companies will have at least one person with cybersecurity and personal data security skills and experience, indicating the need to build trust and confidence among consumers and businesses to drive the growth of the digital economy.

Looking at the Indonesian context, based on the Google Tamasek report (2024), it shows that the domestic internet penetration rate in early to mid-2024 reached 79.5%. The ratio of the population connected to the internet has reached 79.5% of the total national

[1] Blume, P. (1998). Data protection of law offenders. Information, Communication & Society, 1(4), 442–466

[2] Koops, B.-J. (2014). The trouble with European data protection law. International Data Privacy Law, 4(4), 250–261

[3] Moerel, L. (2010). The long arm of EU data protection law- Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? International Data Privacy Law, 1(1), 28–46.

[4] Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 2). International Journal of Law and Information Technology, 18(3), 227–247

[5] Charlesworth, A. (1999). Implementing the European union data protection directive 1995 in UK law- The data protection act 1998. Government Information Quarterly, 16(3), 203–240.

[6] OECD (2024), OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier, OECD Publishing, Paris, https://doi.org/10.1787/a1689dc5-en.

[7] UN Digital Economy Report (2024) : Digital Economy Report 2024 Shaping an environmentally sustainable and inclusive digital future, UNCTAD Publishing, United Nations publication issued by the United Nations Conference on Trade and Development, ISBN: 978-92-1-003136-3, eISBN: 978-92-1-358977-9, EPUB ISBN : 978-92-1-358978-6 ISSN: 2664-2255, eISSN: 2664-2263. https://unctad.org/system/files/official-document/der2024_en.pdf

population. Indonesia's internet penetration rate has been recorded as continuing to increase every year, reaching a new record high in mid-2024. However, the distribution of penetration is not yet even. However, it is necessary to be seriously concerned that the distribution of internet access in Indonesia is not yet even. Java Island has the highest internet penetration rate, namely 83.64%, followed by Kalimantan (77.42%) and Sumatra (77.34%). On the other hand, Maluku and Papua have the lowest internet penetration rates, namely 69.91%. Overall, the data shows that although internet access in Indonesia continues to increase, there is still a digital divide between regions. Continuous efforts are needed to ensure equitable and affordable internet access for all Indonesians.

Before the privacy law, Indonesia used the ITE Law No. 11 of 2008 (which revised twice namely: Law No. 19 of 2016 and Law No. 1 of 2024) as recognition and respect for the rights and freedoms of other people and to fulfill demands that are fair and by considerations of security and public order in Indonesia. Unfortunately, the ITE Law is often misused by some people and even some articles in the ITE Law are also called rubber articles because these articles can also be easily used to ensnare people to silence criticism.

There are several factors that cause the public to demand that the judiciary (DPR) immediately accelerate the draft PDP law so that it is passed into law. Among them are the personal rights of the public which are often violated, whether from misuse of personal data, leakage of personal data, etc.

It has been more than 20 years since technology entered human life. Most technologies today use users' personal data, even for simple applications. As a result, a lot of personal data is collected and combined by several service providers. Sometimes some companies misuse personal data to carry out marketing techniques. That is why the PDP Law provides guarantees for the protection of subject rights.

Privacy compliance for government institutions, companies and organisations is very important to ensure the protection of fundamental rights. PRIVASIMU, a privacy advisory and technology company, provides a tool for PDP readiness assessment. There are 18 questionnaires facilitated for organisations in checking their own readiness assessment. There are about 373 companies which have already filled the form and average compliance score is about less than 35 %. Some companies obtained less than 10 % and the others up to 90 %.

In this article, the author will also discuss several strategies that can be used as references for organizations or the private sector, especially from a risk management perspective.

**Personal Data Mapping**

Most companies do not have information concerning data privacy mapping either customer data privacy map or employee. Which data privacy categories are they processed? Is that a specific data privacy such as biometric, genetic, health data and so on? where the location and whose section is responsible for these data privacy processing?

Data mapping is very important to be defined within organizations. Organization also has to make sure that the ecosystem and third parties are ready to comply with PDP Law as well.[8] In many cases, data privacy processing activities are also displayed by other parties. Therefore organizations should be careful to decide in collecting data privacy[9] and make arrangements with third parties. Moreover, in specific categories of data privacy, the protection and attention should be more careful.[10]

The use of the terminology "personal data" has been explained in Article 1 of the PDP Law, which reads: "Personal Data is data about natural persons who are identified or can be identified individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems."

Some personal data may have “sensitive” content, this data requires special treatment like encryption or masking. Anyone who collects personal data must consider the needs of “why they collect the data?” and they have to consider data subject rights.

In PDP Law personal data has been classified into 2 types of data: general and specific. General data includes categories as:

- Full Name
- Gender
- Nationality
- Religion
- Marriage status
- Personal data combined for identification of persons

Sensitive data includes categories as:

- Health data and information

[8] Bossi. (2002). European Directive of October 24, 1995 and Protection of Medical Data- The Consequences of the French Law Governing Data Processing and Freedoms. European Journal of Health Law, 9(3), 201–206.

[9] Azmi, I. M. (2007). Personal data protection law- The Malaysian experience. Information & Communications Technology Law, 16(2), 125–135

[10] Chalton, S. (1997). The Transposition into UK Law of EU Directive 95/46/EC (the Data Protection Directive). International Review of Law, Computers & Technology, 11(1), 25–32.

- Biometric data
- Generic data
- Criminal record
- Child data
- Financial data
- Other data is following the provisions of the Law

When data is requested, the bulk of the data gathered about individuals is collected and must be disclosed in the company's privacy statement. The privacy statement explains the personal data processes, how the data controller processes it, and for what purposes. This privacy notice is a part of transparency which shows a good will of the controller on how they are processing the data privacy. Most organisations already have a privacy notice and inform the public what kind of data privacy that they are processing. However, some organisations do not have this privacy notice. Before October 2024, they have to publish a privacy notice to make sure that they are trying to comply with PDP Law.
Furthermore, they have to make and revise their own classification data policy. Most organisations have a classification data policy such as category of data ranging from secret data, limited data and public data, etc. With PDP Law, the classification data policy will be added with these ordinary data privacy and sensitive data privacy as well.

**The Power of Data Subject**

Before Law No. 27 of 2022 concerning privacy data protection, people were just only an object of data. After this Law is enacted, individuals transform from data objects to become data subjects. They have several rights such as right to access, revoke, edit, delete, postpone, etc. Government institutions, mostly, do not have a channel to data subject in requesting their rights. However, Banking, E-commerce, Telecommunication Companies, etc do have a Data Subject Access Request (DSAR). This mechanism of DSAR is very important to respect the rights of data subjects.
In Article 1 of PDP Law, Data Subject means "the individual to whom the Personal Data is attached.". The rights of data subjects are regulated in articles 5 to 15, including the right to obtain information about the clarity of identity, the basis of legal interests, the purpose of requesting and using personal data, and the accountability of the party requesting personal data, the right to end processing, delete and/or destroy personal data about him, and has the right to sue and receive compensation for violations of the processing of personal data about him.

But, according to article 15 paragraph 1 said:
The rights of Personal Data Subjects as intended in Article 8, Article 9, Article 10 paragraph (1), Article 11, and Article 13 paragraph (1) and paragraph (2) are excluded for:

1. National defense and security interests;
2. Interests in the law enforcement process;
3. Public interest in the context of state administration;
4. Interests in the supervision of the financial services sector, monetary, payment systems and financial system stability carried out in the context of state administration; or
5. interests in statistics and scientific research.

**The Obligation of Data Controllers**

A Data Controller is anyone, public agency, or international organization who acts individually or jointly in determining the purposes and exercising control over the processing of personal data.
A Data Controller must have a basis for processing Personal Data, which means:

1. Carrying out explicit legal consent from the Personal Data Subject for 1 (one) or several specific purposes that have been conveyed by the Personal Data Controller to the Personal Data Subject.
2. Fulfillment of contractual obligations if the Personal Data Subject is a party or to fulfill the request of the Personal Data Subject when agreeing.
3. Fulfillment of the legal obligations of the Personal Data Controller by statutory provisions.
4. Fulfilling the protection of the vital interests of Personal Data Subjects.
5. Carrying out duties in the public interest, public service, or exercising the authority of the Personal Data Controller based on statutory regulations; and/or.
6. Fulfillment of other legitimate interests by taking into account the objectives, needs, and balance of interests of the Personal Data Controller and the rights of the Personal Data Subject.

In Data Processing, A Data Controller must convey information regarding the legality of the processing of Personal Data; purposes of processing Personal Data; the type and relevance of Personal Data to be processed; the retention period for documents containing Personal Data; details regarding the Information collected; period of processing of Personal Data; and the rights of Personal Data

Subjects. If there is a change in information, the Data Controller must notify the Personal Data Subject before any modifications to the Information occur.

**The Existence of Data Protection Officer**

A Data Protection Officer is an official or officers who carry out PDP functions. DPO is a profession that was created by the PDP Law. Every company must appoint a DPO to monitor data processing regularly and on a large scale. Even though the DPO is appointed by the company, the PDP Law stipulates that the DPO's position is independent. The main task of the DPO is to ensure that companies comply with the provisions of the PDP Law.

**Difference with GDPR**

According to APTIKA, even though drafting the PDP Bill refers to the GDPR, there are differences in the components of the PDP Bill and the GDPR, namely as follows:

**Table 1, PDP and GDPR differences**

| | PDP | GDPR |
|---|---|---|
| Exceptions to the rights of data owners | **In full**, based on several areas of interest regulated in the PDP Law | **Partially**, based on the principles of necessity and proportionality |
| Limitations on storage of personal data | It can be extended as long as it meets the law | It can be extended for some specific needs |
| Personal data controller obligations | Set Generally regardless of high or low processing risk | DPIA applies to high-level processing |
| Personal data processor obligations | Some obligations of the data controller also become obligations of the data processor | Some data controller obligations are different from data processor obligations |
| The need for personal data security | Regulates generally based on the capacity that will be applied in derivative legislation | Based on the capacity and competence of the controller/processor |
| Cross-border data transfer | 3 aspects are the same as GDPR, but do not have to be followed step by step | The 3 aspects of cross country must be followed in stages |
| Penalty or Punishment | administrative sanctions for negligence in obligations, and criminal sanctions for prohibited misuse | only regulates administrative sanctions |
| The Authority of Privacy Law | the authority is independent | the authority body is independent according to every country in Europe |

**Source:** APTIKA KOMINFO

**Personal Data Protection from a Risk Management Perspective**

Some important aspects in personal data protection from a risk management perspective are *firs*t Information lifecycle management (ILM). It is also often equated with data lifecycle management (DLM), a set of rules created and used by organizations or companies using tools (software) to comply with data processing policies. Tom Petrocelli (2005) the DLM process carefully considers what information or data is owned, where it is located, what relationships it has with other information, and the life cycle of the information[11].

Data lifecycle management creates a framework for managing data from creation, storage, archiving, to disposal. These activities are often considered a fundamental component of a data protection strategy and should be reviewed periodically to ensure ongoing and planned data protection activities are aligned with the data lifecycle and business processes.

*The second* aspect is Data loss prevention (DLP) which refers to the strategies or methods, processes, and technologies used by cyber security teams in an organization or company to protect sensitive data from theft, loss, and misuse. Data loss is often described as a data breach, data leakage, or data exfiltration. The terms are sometimes used interchangeably but have different meanings. A data breach is a cyberattack or other security incident that results in unauthorized access to sensitive data or confidential information.

[11] Tom Petrocelli (2005), Data Protection and Information Lifecycle Management, September 23, 2005 Published by Prentice Hall, ISBN 9780131927575 (ISBN10: 0131927574

This includes personal data (e.g., passport numbers, social security, bank account numbers, healthcare data) or corporate data (e.g., customer records, intellectual property, financial data). According to the IBM Cost of a Data Breach 2023 report, the average breach costs $4.45 million, a 15 percent increase over the past three years.

*The third* aspect is data risk management. According to Alexander Borek et al (2014) Data risk management is a series of processes to identify and assess risks and threats to data that are very important when formulating most aspects of a data protection strategy, because this strategy aims to minimize the possibility of risks occurring and to mitigate the severity of events that have a negative impact on data[12].

To provide a comprehensive and comprehensive understanding of how to map data risk management and understand data asset management, companies or organizations can start by trying to see a very comprehensive reference by looking at the Risk Management Framework (RMF) formulated by the National Institute of Standard and Technology (NIST). NIST RMF is a framework used to help organizations understand and determine their security and risk management activities. There are seven steps in RMF: prepare, categorize, selection of security controls, implementation of controls, assessment, authorization of a system for use, and finally monitoring of the selected controls[13].

Privacy risk assessments can help organizations understand in a context the privacy values that must be protected, the methods applied, and how to balance the application of different types of actions or data processing.

As an additional conclusion, privacy risk assessments can help organizations or companies to distinguish between privacy risk and compliance risk. Privacy risk assessments should be able to identify whether data processing can cause problems for individuals, even when an organization may be fully compliant with applicable laws (PDP/GDPR) or regulations, can help make ethical decisions in the design or implementation of systems, products, and services

## CONCLUSION

The PDP Law clarity is a major step forward for enhancing data privacy in Indonesia, harmonizing data protection rules, and promoting privacy and security as core aspects of Cybersecurity and Privacy in every sector of industry. The PDP Law can become a legal umbrella to protect the rights and obligations of data owners, business actors, and data exchange processes with other countries.

## REFERENCES


1) Alexander Borek et al (2014), In praise of Total Information Risk Management: Maximizing the Value of Data and Information Assets, organ Kaufmann, 2014, ISBN 9780124055476, https://doi.org/10.1016/B978-0-12-405547-6.05001-X. (https://www.sciencedirect.com/science/article/pii/B978012405547605001X)
2) Annan, Alaikha. "TINJAUAN YURIDIS PERLINDUNGAN DATA PRIBADI PADA SEKTOR KESEHATAN BERDASARKAN UNDANG-UNDANG NO. 27 TAHUN 2022." Synergy: Jurnal Ilmiah Multidisiplin 1, no. 04 (2024): 247-254.
3) APTIKOM KOMINFO. “Urgensi General Data Protection Regulation (GDPR) di Indonesia”, (2020).
4) Azmi, I. M. (2007). Personal data protection law- The Malaysian experience. Information & Communications Technology Law, 16(2), 125–135
5) Baxevani, Theodora. "GDPR Overview." (2019).
6) Bintarawati, Fenny. "THE INFLUENCE OF THE PERSONAL DATA PROTECTION LAW (UU PDP) ON LAW ENFORCEMENT IN THE DIGITAL ERA." ANAYASA: Journal of Legal Studies 1, no. 2 Januari (2024): 135-143.
7) Blume, P. (1998). Data protection of law offenders. Information, Communication & Society, 1(4), 442–466.
8) Bossi. (2002). European Directive of October 24, 1995 and Protection of Medical Data- The Consequences of the French Law Governing Data Processing and Freedoms. European Journal of Health Law, 9(3), 201–206.
9) Chalton, S. (1997). The Transposition into UK Law of EU Directive 95/46/EC (the Data Protection Directive). International Review of Law, Computers & Technology, 11(1), 25–32.
10) Charlesworth, A. (1999). Implementing the European union data protection directive 1995 in UK law- The data protection act 1998. Government Information Quarterly, 16(3), 203–240.
11) Koops, B.-J. (2014). The trouble with European data protection law. International Data Privacy Law, 4(4), 250–261
12) Korpisaari, Paivi. "Finland: A brief overview of the GDPR implementation." Eur. Data Prot. L. Rev. 5 (2019): 232.
13) Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (Part 2). International Journal of Law and Information Technology, 18(3), 227–247.


[12] Alexander Borek et al (2014), In praise of Total Information Risk Management: Maximizing the Value of Data and Information Assets, organ Kaufmann, 2014, ISBN 9780124055476, https://doi.org/10.1016/B978-0-12-405547-6.05001-X. (https://www.sciencedirect.com/science/article/pii/B978012405547605001X)

[13] To see details of the Risk Management Framework (RMF), please visit the following link: https://csrc.nist.gov/projects/risk-management/about-rmf

14) Moerel, L. (2010). The long arm of EU data protection law- Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide? International Data Privacy Law, 1(1), 28–46.
15) OECD (2024), OECD Digital Economy Outlook 2024 (Volume 1): Embracing the Technology Frontier, OECD Publishing, Paris, https://doi.org/10.1787/a1689dc5-en.
16) Tom Petrocelli (2005), Data Protection and Information Lifecycle Management, September 23, 2005 Published by Prentice Hall, ISBN 9780131927575 (ISBN10: 0131927574.
17) Undang-Undang Nomor 27 Tahun 2022: Pelindungan Data Pribadi.
18) UN Digital Economy Report (2024) : Digital Economy Report 2024 Shaping an environmentally sustainable and inclusive digital future, UNCTAD Publishing, United Nations publication issued by the United Nations Conference on Trade and Development, ISBN: 978-92-1-003136-3, eISBN: 978-92-1-358977-9, EPUB ISBN : 978-92-1-358978-6 ISSN: 2664-2255, eISSN: 2664-2263. https://unctad.org/system/files/official-document/der2024_en.pdf.