The Indonesian Journal of International Clinical Legal Education
Vol. 6 Issue 1 (2024) 111–150
DOI: https://doi.org/10.15294/ijicle.v6i1.2002
Available online since: March 31, 2024

The Indonesian Journal of
International Clinical
Legal Education
https://journal.unnes.ac.id/sju/index.php/iccle/index

Data Protection Impact Assessment Indicators in Protecting Consumer Personal Data on E-commerce Platforms

Tegar Islami Putra
Faculty of Law Universitas Negeri Semarang, Semarang, Indonesia, tegarislami44@students.unnes.ac.id

Nurul Fibrianti ✉
Faculty of Law Universitas Negeri Semarang, Semarang, Indonesia, nurulfibrianti@mail.unnes.ac.id

Mohammad Raziq Fakhrullah
Faculty of Civil Engineering, Universiti Teknologi Malaysia, Malaysia

✉ Corresponding email: nurulfibrianti@mail.unnes.ac.id

Abstract

Efforts to protect consumers' personal data on e-commerce platforms can be carried out by conducting a Data Protection Impact Assessment. This article discusses the indicators of the execution of Data Protection Impact Assessment by pivoting on the rights of personal data subjects based on Law Number 27 of 2022. This research uses a library research method by focusing on legal materials so that it can be said to be library based. The results show that Data Protection Impact Assessment is explained in Article 34 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection which is then further regulated through Government Regulations as mandated by Article 34 paragraph (3). However, the Government Regulation relating to this matter has not yet been ratified, so it still refers to the mandate of Law Number 27 of 2022. This Data Protection Impact Assessment indicator can refer to Article 16 paragraph (2), Article 34 paragraph (1) and (2), Article 35, Article 20 paragraph (2), and Article 27 of Law Number 27 Year 2022. In terms of Data Protection Impact Assessment indicators as the protection of consumer personal data on e-commerce platforms, it can refer to the mandate that explains the rights of personal data subjects and their limitations in a separate article and the form of personal data processing as mandated by Article 34 paragraph (2) of Law No. 27 of 2022.

Keywords

Indicators; Data Protection Impact Assessment; Consumer Personal Data; E-Commerce.

Submitted: 26/07/2023 **Revised:** 29/08/2023; 11/09/2023 **Accepted:** 17/09/2023

I. Introduction

The protection of personal or private rights will increase human values, improve the relationship between individuals and their communities, increase independence or autonomy to exercise control and obtain decency, and increase tolerance and keep away from discrimination and limit government power.[1] Data protection can basically relate specifically to privacy as stated by Allan Westin who for the first time defined privacy as the right of individuals, groups or institutions to determine whether or not information about them will be communicated to other parties so that the definition put forward by Westin is called information privacy because it involves personal information.[2] The data is called a digital dossier, which is a collection of personal data information owned by most or even almost all people by utilizing internet technology developed by private parties, which is very risky for violating the right to privacy of one's personal data.[3] E-

[1] Danrivanto Budhijanto, Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi (2010). p.4. Id. p.4.

[2] Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," Jurnal Yuridis 7, no. 1 (2020): p.107, https://doi.org/10.35814/selisik.v6i1.1699. Hanifan Niffari, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)," Jurnal Yuridis 7, no. 1 (2020): p.107, https://doi.org/10.35814/selisik.v6i1.1699.

[3] Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum," Jatiswara 34, no. 3 (2019): 243. Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum," Jatiswara 34, no. 3 (2019): 243.

Commerce as a platform that utilizes internet technology and connects users with each other, is basically a platform that indirectly manages the personal data of platform users.

E-Commerce is the process of trade transactions, be it goods, services, or information using the internet network.[4] E-commerce companies must ensure that customers' personal data is secure and well-protected to maintain customer trust and build strong and lasting relationships with them.[5] In the e-Conomy SEA 2023 report, it is stated that the outlook for the gross transaction value of e-commerce in 2023 is US$ 62 billion, growing 7% on an annual basis (YoY).[6] Indonesia's e-commerce market is expected to be a major growth contributor in Asia Pacific. Based on RedSeer analysis, Indonesia's e-commerce market is projected to increase to US$137.5 billion by 2025.[7] This figure is the impact of the ease of e-commerce practice itself. E-commerce practices can improve the country's economy because it saves transaction costs, eliminates time and space constraints, reduces shipping

[4] S. S Dhaka, Impact Od Growing E-Commerce on Indian Farmers, 13 Indian J Econ Dev 596 (2017). Id.

[5] Khafidah Puspita, "Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia," Jurisprudensi : Jurnal Ilmu Syariah, Perundangan-Undangan Dan Ekonomi Islam 15, no. 1 (2023): 47, https://doi.org/10.32505/jurisprudensi.v15i1.5478.

[6] Anna Suci Perwitasari, Google CS Ungkap Alasan Potensi Perlambatan Pertumbuhan Penjualan E-Commerce, Kontan.co.id2 (2023). Id.

[7] Reza Pahlevi, Nilai Transaksi E-Commerce Indonesia Diperkirakan Capai US$137,5 Miliar Pada 2025, Databoks.katadata.co.id (2022), https://databoks.katadata.co.id/datapublish/2022/03/18/nilai-transaksi-e-commerce-indonesia-diperkirakan-capai-us1375-miliar-pada-2025 (last visited Feb 21, 2024). Id.

costs, minimizes transportation barriers, facilitates seller and buyer communication, and reduces advertising and transportation costs.[8]

According to Zheng Qin in his book Introduction to E-Commerce, when conducting and accepting online transactions, it is necessary to provide consumers' personal data.[9] The high number of e-commerce users is supported by easy registration requirements on the marketplace, which is enough to register using an Identity Card, telephone number, e-mail.[10] E-commerce is a business activity that deals with consumers, manufacturers, service providers, and intermediaries using computer networks, i.e. e-commerce has covered the entire spectrum of commercial activities.[11] In addition, e-commerce transactions involve parties, namely sellers (merchants), buyers (card holders), billing intermediaries (acquirers), credit card issuers (issuers),

[8] Rais Agil Bahtiar, Potensi, Peran Pemerintah, Dan Tantangan Dalam Pengembangan E-Commerce Di Indonesia [Potency, Government Role, and Challenges of E-Commerce Development in Indonesia], 11 J Ekon dan Kebijak Publik 13 (2020). Id.

[9] Etania Fajarani Halim, Perlindungan Hukum Data Pribadi Pembeli Di Perdagangan Secara Elektronik (E-Commerce) Di Indonesia, 2 J Huk Visio Justisia 1 (2022), https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_233321.aspx. Id.

[10] Bram Freedrik Sangojoyo, Aurelius Kevin & David Brilian Sunlaydi, Urgensi Pembaharuan Hukum Mengenai Perlindungan Data Pribadi E-Commerce Di Indonesia, 22 Kosmik Huk 27 (2022). Id.

[11] Niniek Suparni, Cyberspace Problematika & Antisipasi Pengaturannya (2009). Id.

certification authorities, and shipping or expedition services, then all of these parties are also called e-commerce users.[12]

To ensure the protection of consumers' personal data, it is imperative to establish clear and robust legal protections. These legal protections aim to maintain the confidentiality, security and integrity of consumers' personal information. The responsibility for designing these personal data protection strategies lies with the government or state authorities. As the more vulnerable party in e-commerce transactions, consumers need guarantees regarding their rights in economic activities.[13] To guarantee the privacy rights of citizens, Indonesia has passed a regulation on personal data protection through law. Law No. 27 of 2022 on Personal Data Protection was passed by the President of the Republic of Indonesia on October 17, 2022 with the main objective of protecting the personal data of the public managed by electronic system administrators (PSE), such as the Ministry of Communication and Information of the Republic of Indonesia, as well as preventing crimes committed by irresponsible individuals.[14] In the general explanation, Law Number 27 Year 2022 explains

[12] Dianne Eka Rusmawati, Perlindungan Hukum Bagi Konsumen Dalam Transaksi E-Commerce, 7 Justisia J Ilmu Huk 195 (2013). Id.

[13] Sagdiyah Fitri Andani Tambunan Agung & Muhammad Irwan Padli Nasution, Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Di E-Commerce, 2 J Ekon Manaj dan Bisnis 5 (2023). Id.

[14] Muhammad Yudistira & Ramadhan, Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo, 5 Unes Law Rev 3802 (2023), https://doi.org/10.31933/unesrev.v5i4. Id.

that Personal Data Regulation aims, among others, to protect and guarantee the basic rights of citizens related to personal protection, guarantee the public to get services from Corporations, Public Bodies, International Organizations, and the Government, encourage the growth of the digital economy and the information and communication technology industry, and support the improvement of domestic industry competitiveness.

The general regulation of personal data protection is found in Law No. 8/1997 on Company Documents, Law No. 36/1999 on Telecommunications, Law No. 24/2013 on Population Administration, Law No. 19/2016 on Electronic Information and Transactions, Law No. 36/2009 on Health, and Law No. 43/2009 on Archives. However, the study in this paper is limited to the protection of personal data that is directly related to electronic data.[15] For the latest regulation related to personal data, the government issued Law Number 27 Year 2022 on Personal Data Protection.

In personal data protection, there is the term Data Protection Impact Assessment (DPIA). DPIA is basically needed in protecting personal data.[16] DPIAs under the GDPR and Law Enforcement Directive (LED) are based on how risks

[15] Hari Sutra Disemadi, Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia, 5 J Wawasan Yuridika 177 (2021). Id.

[16] Tim Publikasi, FGD Tentang Data Protection Impact Assessment (DPIA) Dalam Pemrosesan Data Biometrik, Atmajaya.ac.id (2023), https://www.atmajaya.ac.id/id/pages/fgd-dpia-lppm/ (last visited Feb 21, 2024). Id.

are managed "ex-ante" before processing, rather than on the harm or impact of data processing. Given the central premise of high risk in DPIAs and the discretion of data controllers in risk management, DPIAs are seen as part of the risk-based approach in EU data protection law.[17] This DPIA itself is one of the accountability efforts of personal data controllers.

Based on the background as stated above, the research questions of this study include: (1) what are the general indicators of Data Protection Impact Assessment to fulfill the mandate of Law Number 27 of 2022? (2) How is the juridical study of Data Protection Impact Assessment indicators in protecting consumer personal data on the E-Commerce Platform based on Law Number 27 of 2022?

II. Method

This research is limited only to the DPIA rules in general by personal data managers on e-commerce platforms and the rights of personal data subjects as mandated by Law Number 27 of 2022. This research aims to find out the indicators in Protecting Consumer Personal Data on E-Commerce Platforms based on the rights of personal data subjects based on Law Number 27 of 2022. The benefits and novelty of this research are that the general public can find out the general

[17] Eyup Kun, Exploring the Role of Data Protection Impact Assessments in the Use of Facial Recognition Technologies: From Accountability to Meta-Regulation, Soc Sci Res Netw (2022), https://dx.doi.org/10.2139/ssrn.4239404. Id.

indicators of DPIA according to Law Number 27 of 2022 and that the public can find out the DPIA Indicators in Protecting Consumer Personal Data on E-Commerce Platforms based on Personal Data Subject Rights according to Law Number 27 of 2022. Scientific research uses one of the grand method sections, namely Library Research which is based on literature or literature. Based on the subject of study and the type of problem at hand, then of the 3 (three) types of grand methods that have been mentioned above, in this research, Library Research or this research will use the Library Research method or library research. Regarding this kind of research, it is also commonly called "Legal Research".[18] This kind of legal research does not recognize field research because what is studied is legal material so that it can be said to be library based, focusing on reading and analysis and analysis of the primary and secondary materials.[19]

[18] Soerjono Soekanto & Sri Mamudji, Penelitian Hukum Normatif Tinjauan Singkat (2006). p.66.

[19] Jhony Ibrahim, Teori Dan Metodologi Penelitian Hukum Empiris (2006). p.98.

III. Result & Discussion

A. General Indicators of Data Protection Impact Assessment Based on Law Number 27 of 2022 as an Effort to Fulfill The Rights of Personal Data Subjects

Some personal data processed is more sensitive and requires higher protection. Under the GDPR, these are known as 'special categories of personal data', and include information about Race Ethnicity Political views Religion, spiritual or philosophical beliefs Biometric data for identification purposes Health data Sex life data Sexual orientation Genetic data.[20] The GDPR was passed in 2016, but only came into effect on May 25, 2018.[21] Referring to the mandate of Art 35 Article 29 GDPR, Data Protection Impact Assessment (DPIA) can be defined as an assessment of the impact on personal data protection of the types of processing taking into account its nature, scope, context and purpose, likely to cause a high risk to the rights and freedoms of individuals. DPIA is a process designed to explain processing, assess its necessity and

[20] Publication Team, Special Categories of Personal Data - GDPR EU, GDPR.EU.org (2020), https://www.gdpreu.org/the-regulation/key-concepts/special-categories-personal-data/ (last visited Feb 24, 2024). Id.

[21] Syafira Agata Ramadhani, "Komparasi Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa," Jurnal Hukum Lex Generalis 3, no. 1 (2022): 79, https://doi.org/10.56370/jhlg.v3i1.173. Syafira Agata Ramadhani, "Komparasi Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa," Jurnal Hukum Lex Generalis 3, no. 1 (2022): 79, https://doi.org/10.56370/jhlg.v3i1.173.

proportionality, and help manage risks to the rights and freedoms of natural persons resulting from the processing of personal data by assessing them and determining measures to address them.[22] DPIA will consist of several questions asked to the deputy or one of the sub-sections of the program organizer in a company or entity as a form of effort to fulfill personal data.

DPIA is used to be able to protect the types of personal data as regulated in Chapter III of Law Number 27 Year 2022. However, the processing of personal data that is required to be carried out DPIA is personal data that has a high risk potential as referred to in Article 34 paragraph (1). Regulations regarding the types of personal data in general are regulated in Article 4 of Law Number 27 of 2022.[23] Referring to the regulation, the classification of personal data consists of specific personal data and general personal data. Specific Personal Data is Personal Data which, if processed, may result in a greater impact on the Personal Data Subject, including acts of discrimination and greater harm to the Personal Data Subject. The classification of specific personal data includes health data and information, biometric data, genetic data, crime records, child data, personal information data; and/or, other data in accordance with the provisions of laws and

[22] Dalla Corte et al., Data Protection Impact Assessment Methods for The Urban Environment, (2022). Id.

[23] Al, Rifqy, Muh et al., "PERLINDUNGAN DATA PRIBADI BAGI PENGGUNA MEDIA SOSIAL," Jurnal Al Tasyri'iyyah 3, no. 2 (2023): p.114.

regulations. Meanwhile, general Personal Data includes full name, gender, nationality, religion, marital status; and/or Personal Data that is combined to identify a person, including cellular telephone number and IP Address.[24]

In Law Number 27 Year 2022, it is not explained how the indicators of DPIA, and it does not even explain DPIA explicitly. However, the meaning of DPIA is in line with the mandate of Article 31 and Article 34 paragraph (1) which indirectly explains that the personal data controller is obliged to record all Personal Data processing activities, and the impact assessment of Personal Data Protection must be carried out by the personal data controller in the event that the Personal Data processing has a high potential risk to the Personal Data Subject. The form of personal data processing itself has been explicitly explained through the mandate of Article 16 paragraph (1). In this case, personal data processing includes:

a) Acquisition and collection;
b) Processing and analyzing;
c) Storage;
d) Improvement and updating;
e) Appearance, announcement, transfer, dissemination, or disclosure; and/or

[24] Kirana Rukmayuninda Ririh et al., "Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum Dan Kebijakan Di Indonesia," Journal Ners 15, no. 2 (2020): p.868. http://journal.universitaspahlawan.ac.id/index.php/ners/article/view/16088.

f) Removal or destruction.

The implementation of personal data processing by the personal data controller itself does not necessarily exist in a vacuum. The implementation of personal data processing must be carried out in accordance with the principles of Personal Data Protection as explained in Article 16 paragraph (2), which includes:

a) Collection of Personal Data is limited and specific, lawful and transparent;
b) Processing of Personal Data is carried out in accordance with its purpose;
c) The processing of Personal Data is carried out by guaranteeing the rights of the Personal Data Subject;
d) The processing of Personal Data shall be accurate, complete, non-misleading, up-to-date, and accountable.

Furthermore, in the explanation of Article 34 paragraph (1), it is explained that DPIA is basically conducted to evaluate the potential risks arising from a processing of personal data as well as the efforts or steps that must be taken to mitigate the risks, including to the rights of Personal Data Subjects and to comply with this Law. This risk mitigation must be implemented in every processing of personal data. In terms of personal data processing, the stages of personal data processing are explained by a cyber law expert from the Faculty of Law, Universitas Airlangga, Masitoh Indriani, S.H., LL.M., that there are at least six stages from obtaining and collecting data, processing and analyzing data, storing data, repairing and updating data, announcing or disseminating data, and deleting or destroying data.[25]

Furthermore, Article 34 paragraph (2) describes the types of personal data that pose a high risk to Personal Data Subjects, which are:

a) automated decision-making that has legal consequences or a significant impact on the Personal Data Subject;
b) processing of Personal Data of a specific nature;
c) processing of Personal Data on a large scale;
d) processing of Personal Data for systematic evaluation, scoring or monitoring activities of Personal Data Subjects;
e) processing of Personal Data for activities of matching or merging a group of data;
f) the use of new technologies in the processing of Personal Data; and/or
g) processing of Personal Data that restricts the exercise of rights of the Personal Data Subject.

For the processing of personal data, the Personal Data Controller also has obligations that need to be considered in terms of processing personal data. Article 35 explains that the

[25] Yuni Afifah, Pakar Hukum Siber UNAIR Jelaskan Prinsip Perlindungan Data Pribadi, fh.unair.ac.id (2023), https://fh.unair.ac.id/pakar-hukum-siber-unair-jelaskan-prinsip-perlindungan-data-pribadi/.

Personal Data Controller is obliged to protect and ensure the security of the Personal Data it processes, by conducting:

a) preparation and implementation of operational technical measures to protect Personal Data from interference with the processing of Personal Data contrary to the provisions of laws and regulations; and
b) determination of the security level of Personal Data by taking into account the nature and risks of the Personal Data to be protected in the processing of Personal Data..

It is also important to note that every Personal Data Controller is obliged to ensure the implementation of personal data protection (including the execution of DPIA) to maintain the accuracy, completeness, and consistency of personal data belonging to personal data subjects in accordance with statutory provisions and accompanied by verification as explicitly mentioned in Article 29 paragraphs (1) and (2). The basis for the processing of personal data by the personal data controller is not done arbitrarily and there are several regulated bases. Processing of personal data must fulfill the provisions of the existence of valid consent in accordance with the purpose of using the data.[26] In addition, every personal data controller in conducting personal data processing is obliged to have a basis for processing personal

[26] Willa Wahyuni, Melihat Prinsip Dan Dasar Pemrosesan Data Pribadi, hukumonline.com (2023), https://www.hukumonline.com/berita/a/melihat-prinsip-dan-dasar-pemrosesan-data-pribadi-lt64a2df2ad70ce/?page=2. Id.

data as mandated by Article 20 paragraph (1). Furthermore, Article 20 paragraph (2) explains that the grounds for processing personal data include:

a) explicit valid consent from the Personal Data Subject for 1 or more specific purposes that has been conveyed by the Personal Data Controller to the Personal Data Subject;
b) fulfillment of an agreement obligation in the event that the Personal Data Subject is a party or to fulfill the request of the Personal Data Subject at the time of entering into an agreement;
c) fulfillment of legal obligations of the Controller of Personal Data in accordance with the provisions of laws and regulations;
d) fulfillment of the protection of the vital interests of the Personal Data Subject;
e) performance of tasks in the context of public interest, public service, or implementation of the authority of the Personal Data Controller based on laws and regulations; and/or.
f) fulfillment of other legitimate interests by taking into account the purposes, needs, and balance of the interests of the Personal Data Controller and the rights of the Personal Data Subject.

It should be underlined that the processing of personal data belonging to personal data subjects managed by personal data controllers must be limited and specific, lawful, and transparent as mandated by Article 27. What is meant by "limited and specific" management of personal data is that the collection of Personal Data must be limited in accordance with the purpose of the processing and the purpose of processing Personal Data must be explicit, lawful, and determined at the time of the Personal Data. Furthermore, what is meant by "legally valid" is that the processing of Personal Data is carried out in accordance with the provisions of laws and regulations. Meanwhile, "transparent" means that the processing of Personal Data is carried out by ensuring that the Personal Data Subject has knowledge of the Personal Data processed and how the Personal Data is processed, and that any information and communication relating to the processing of Personal Data is easily accessible and understandable, using clear language. This has been explicitly explained in the explanation of Article 27.

As explained earlier, DPIA is implicitly stipulated in Article 34 paragraph (1) which reads "The Personal Data Controller shall conduct an impact assessment of Personal Data Protection in the event that the processing of Personal Data has a high potential risk to the Personal Data Subject.". Furthermore, it is explained in paragraph (3) that, "Further provisions regarding the impact assessment of Personal Data Protection shall be stipulated in a Government Regulation". However, the Government Regulation governing the impact assessment of Personal Data Protection has not yet been enacted. So that the DPIA indicators that can currently be used in Indonesia are some of the rules contained in Law Number 27 Year 2022 itself. Some articles and mandates that need to be considered in relation to DPIA are the mandate of

Article 16 paragraph (2) which regulates the principle of Personal Data Protection, Article 34 paragraph (1) and (2) which regulates the scope of Personal Data that has a high potential risk to Personal Data Subjects, Article 35 which explains the actions that must be taken by Personal Data Controllers in protecting and ensuring the security of Personal Data, Article 20 paragraph (2) which explains the basis for processing Personal Data, and Article 27 which explains the management of personal data carried out by personal data controllers in a limited and specific, legally valid, and transparent manner.

B. Indicators of Data Protection Impact Assessment in Protecting Indonesian Consumer Personal Data on E-Commerce Platforms Based on Personal Data Subject Rights in Law Number 27 of 2022

According to Article 1 Point 6 of Law No. 27 of 2022, a personal data subject is an individual to whom personal data is attached.[27] Personal data that is given protection by the state is classified in legislation. Article 4 of Law No. 27 of 2922 has provided a classification of the types of personal data.[28] Article 4 regulates the types of personal data that need to be protected, consisting of specific personal data and general personal data. Specific personal data includes health data and information, biometric data, genetic data, criminal records, child data,

[27] Muhammad Irfan Ilm, Geger Jaka Kiswara, and Syarif Mustika, "PERLINDUNGAN DATA PRIBADI PENGGUNA APLIKASI PADA SMARTPHONE DITINJAU DARI HUKUM POSITIF," Nusantara: Jurnal Ilmu Pengetahuan Sosial 9, no. 4 (2022): p.2296.. Muhammad Irfan Ilm, Geger Jaka Kiswara, and Syarif Mustika, "PERLINDUNGAN DATA PRIBADI PENGGUNA APLIKASI PADA SMARTPHONE DITINJAU DARI HUKUM POSITIF," Nusantara: Jurnal Ilmu Pengetahuan Sosial 9, no. 4 (2022): p.2296..

[28] Dewi Sulistianingsih et al., "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)," Masalah-Masalah Hukum 52, no. 1 (2023): p.103, https://doi.org/10.14710/mmh.52.1.2023.97-106. Dewi Sulistianingsih et al., "Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi)," Masalah-Masalah Hukum 52, no. 1 (2023): p.103, https://doi.org/10.14710/mmh.52.1.2023.97-106.

personal financial data, and/or other data in accordance with applicable laws. Whereas general personal data includes full name, gender, nationality, religion, marital status and/or personal data combined to identify a person.[29] The management of personal data belonging to consumers in e-commerce is related to the principle of Fair Information Practices (FIP). The United States Privacy Act of 1974 is technically the first implementation of the FIP principle in the world.[30] This FIP principle is partly based on the right to privacy as described in the Harvard Law Review in 1890 by Louis Brandeis and Samuel Warren.

In e-commerce transactions, there are basically consumers who purchase goods. Indirectly, consumers in e-commerce transactions are also subjects of personal data. The management of personal data belonging to consumers in e-commerce is related to the theory of consumer privacy by Garfinkel & Russell which pivots on an activist perspective.[31] The Consumer Privacy Theory proposed by Garfinkel & Russell explains that if free market forces and technological advances are left unchecked, then information will be available

[29] Suyatno, "Analisa Perlindungan Data Pribadi Pengguna Fintech Berdasarkan Pendekatan Yuridis Normatif Di Indonesia.," YUME: Journal of Management 5, no. 3 (2022): p.487, https://doi.org/10.37531/yume.vxix.325. Suyatno, "Analisa Perlindungan Data Pribadi Pengguna Fintech Berdasarkan Pendekatan Yuridis Normatif Di Indonesia.," YUME: Journal of Management 5, no. 3 (2022): p.487, https://doi.org/10.37531/yume.vxix.325.

[30] Robert Gellman, Willis Ware's Lasting Contribution to Privacy: Fair Information Practices, 12 IEEE Secur Priv 51 (2014). Id.

[31] Mary J. Culnan & Robert J. Bies, Consumer Privacy: Balancing Economic and Justice Considerations, 59 J Soc Issues 323 (2003). Id.

to anyone for any purpose, which will violate the right to privacy and cause harmful social impacts on society.[32] Through this, it is then necessary to assess the management of consumer personal data as a form of fulfillment of the privacy of e-commerce service users. One form of this fulfillment can be outlined through the implementation of DPIA.

As previously stated, Article 34 paragraph (3) of Law Number 27 Year 2022 has explained that the impact assessment of personal data protection or DPIA is further regulated in a Government Regulation. However, the Government Regulation governing the impact assessment of Personal Data Protection has not yet been passed. Therefore, the DPIA indicators that can currently be used in Indonesia are some of the mandates contained in Law No. 27 of 2022 itself. Padahal, diperlukan suatu peraturan pelaksana dan pemberlakuan harmonisasi peraturan. This form of harmonization is an indispensable balancing principle to address distortions in both inputs and outputs and make the necessary corrections to restore a fair and balanced relationship (justice for all).[33] The Constitutional Court upheld the right to privacy as part of personal data protection in Decision Number 20/PUU-XIV/2016. However, data protection and

[32] S Garfinkel, Database Nation: The Death of Privacy in the 21st Century (California: O'Reilly Media, Inc, 2000): S Garfinkel, Database Nation: The Death of Privacy in the 21st Century (California: O'Reilly Media, Inc, 2000):

[33] Tegar Islami Putra, The Analysis of the Legal Protection of Ship's Crew in Sea Work Agreement in Indonesia, 5 Indones J Advocacy Leg Serv 181 (2023), https://doi.org/10.15294/ijals.v5i2.75367. p.182.

privacy are two different concepts. The right to personal data protection is a human right, and falls under the right to privacy, including information privacy and data privacy, according to Constitutional Court Decision No. 5/PUU-VIII/2011. The right to privacy is also protected by international legal treaties as a human right. Customers must provide personal information such as full name, phone number, and other relevant details to register on e-commerce platforms. Customers may be asked to upload a photo of their identity card (Kartu Tanda Penduduk, KTP), a selfie with their KTP, or a digital signature in certain situations. These components of personal data need to be protected.[34]

In the implementation of personal data protection by personal data controllers, it is necessary to conduct DPIA as a form of effort to protect and ensure the security of Personal Data processed as mandated by Article 35 of Law Number 27 of 2022. In this case, it certainly also applies to e-commerce service provider companies that manage personal data belonging to consumers as personal data subjects. For a personal data subject, there are rights to the management of personal data. These rights of personal data subjects are regulated in Law No. 27 of 2022 in different Articles. However, in general, the rights attached to Personal Data Subjects are described in Article 5 of Law No. 27 of 2022 which states that personal data subjects have the right to obtain

[34] Pohan and Nasution, supra note 5.. p.46.

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.[35]

The rights of personal data subjects are further explained in Articles 6 to 16 of Law No. 27 of 2022. Furthermore, the first personal data subject right is that the personal data subject has the right to complete, update, and/or correct errors and/or inaccuracies in personal data about him/her in accordance with the purposes of personal data processing (Article 6). The second personal data subject right is to obtain access to and obtain a copy of personal data concerning him/her in accordance with the provisions of laws and regulations (Article 7). The third personal data subject right is that the personal data subject has the right to end the processing, erase, and/or destroy personal data about him/her in accordance with the provisions of laws and regulations (Article 8). The fourth personal data subject right is that the personal data subject has the right to withdraw the consent to the processing of personal data concerning him/her that has been given to the personal data controller (Article 9). The fifth personal data Subject Right is that the personal data subject has the right to object to decision-making measures based solely on automated processing, including profiling, which give rise to legal consequences or have a significant impact on the personal data subject (Article 10). The sixth personal data Subject Right is that the personal data subject has the right to delay or restrict processing of personal data in a manner proportionate to the

[35] Egidius Patnistik, Hak-Hak Setiap Subyek Data Pribadi Yang Perlu Dipahami, Kompas.com (2022), https://www.kompas.com/tren/read/2022/12/20/110721965/hak-hak-setiap-subyek-data-pribadi-yang-perlu-dipahami?page=all (last visited Feb 25, 2024). Id.

purposes of the processing of personal data (Article 11). The seventh personal data subject's right is to file a lawsuit and receive compensation for violations of personal data processing about him in accordance with the provisions of laws and regulations.

Further provisions regarding violations of personal data processing and procedures for the imposition of compensation are regulated in government regulations (Article 12). The eighth personal data subject right is that the personal data subject has the right to obtain and/or use personal data about him/her from the personal data controller, in a form that is in accordance with a commonly used structure and/or format, or can be read by an electronic system and the personal data subject has the right to use and transmit personal data about him/her, to other personal data controllers, as long as the systems used can communicate with each other securely, in accordance with the principles of personal data protection, based on Law No. 27 of 2022 (Article 13).

However, the implementation of the rights of personal data subjects in Law Number 27 of 2022 as mentioned above has limitations which are regulated in Article 15 paragraph (1) and paragraph (2) of Law Number 27 of 2022. That the rights of Personal Data Subjects as referred to in Article 8, Article 9, Article 10 paragraph (1), Article 11, and Article 13 paragraph (1) and paragraph (2) are excluded in the context of implementing the provisions of the Law for:

a) the interests of national defense and security;
b) the interests of the law enforcement process;
c) public interest in the context of state administration;

d) the interests of supervision of the financial services sector, monetary, payment system, and financial system stability carried out in the context of state administration; or

e) statistical and scientific research interests.

To fulfill the rights of personal data subjects, the preparation of DPIA by e-commerce platform provider companies must be able to accommodate the rights of personal data subjects as stated above which are then used as indicators in the preparation of DPIA as an effort to protect consumer personal data. This effort is made to avoid misuse and bad possibilities that occur in the management of personal data. Personal data becomes one of the important issues in e-commerce management. This is because personal data is related to the confidentiality and protection of personal data.[36] Personal data is at risk of being compromised and can be used to commit fraud through phishing, spam or malicious software (malware) methods. Therefore, DPIA must also be able to consider the risks that may occur in the management of consumer personal data as a form of personal data processing. Article 34 paragraph (2) of Law Number 27 Year 2022 explains that the processing of personal data through DPIA includes:

a) automated decision-making that has legal consequences or a significant impact on the Personal Data Subject;

b) processing of Personal Data of a specific nature;

c) processing of Personal Data on a large scale;

[36] R Nafiah, Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce, 3 Cyber Secur dan Forensik Digit 18 (2020). Id.

d) processing of Personal Data for systematic evaluation, scoring or monitoring activities of Personal Data Subjects;
e) processing of Personal Data for activities of matching or merging a group of data;
f) use of new technology in the processing of Personal Data; and/or
g) processing of Personal Data that restricts the exercise of rights of the Personal Data Subject.

The application of Data Protection Impact Assessment in order to protect the personal data of personal data subjects also applies to other countries that have a focus and role to protect the personal data of their people. For countries in Southeast Asia, Singapore is one of the first countries to provide a legal umbrella for the protection of personal data for its people. Singapore's PDPA (Personal Data Protection Act) 2012 has been in effect since 2014. This regulation is largely adopted from the European Data Protective Directive (EUDP). In article 5 of the law, there is a body that specifically handles personal data protection, namely the Personal Data Protection Commission (PDPC)..[37] Melalui PDPC, kemudian diterbitkanlah Panduan Penilaian Dampak Perlindungan Data. Panduan ini memberikan garis besar pengantar tentang prinsip-prinsip utama dan pertimbangan untuk organisasi, terutama yang tidak memiliki tindakan atau alat untuk mengatasi risiko perlindungan data pribadi tertentu, dalam melakukan DPIA untuk sistem dan proses.

[37] Publication Team. (2022). Perbandingan Pengaturan Mengenai Otoritas Independen Pada PDPA 2012 Singapura dan PIPA 2011 Korea Selatan. Heylaw.Id. https://heylaw.id/blog/perbandingan-pengaturan-mengenai-otoritas-independen-pada-pdpa-2012-singapura-dan-pipa-2011-korea-selatan.%0A%0A.

Praktik-praktik yang disarankan dalam panduan ini adalah untuk informasi umum dan tidak lengkap.

In these guidelines, explain that DPIAs can be performed on systems (e.g. public-facing websites, cloud storage platforms, Customer Relationship Management ("CRM") systems) and processes (e.g. undergoing a medical examination and receiving a medical report, purchasing goods from an online portal and receiving them from a courier). Key tasks within DPIA that are also indicators of DPIA implementation include:

a) Identifying the personal data handled by the system or process, as well as the reasons for collecting the personal data;
b) Identifying how the personal data flows through the system or process;
c) Identifying data protection risks by analysing the personal data handled and its data flows against PDPA requirements or data protection best practices;
d) Addressing the identified risks by amending the system or process design, or introducing new organisation policies; and
e) Checking to ensure that identified risks are adequately addressed before the system or process is in effect or implemented

In Singapore personal data protection, Individual DPIAs should be conducted for each system or process that involves the handling of personal data (including the linking or sharing of personal data with other parties). For the purpose of this guide, the term "projects" will be used to refer to such systems or processes. It is also recommended that a DPIA be conducted for multiple projects that are similar in purpose, scope and context. For instance, a retail organisation that intends to digitise the collection of consumer data across all its branches may conduct one DPIA exercise that covers the handling of consumers' personal data across branches. Data protection risks are best addressed when the system or process is new and in the process of being designed or in the process of undergoing major changes. Introducing changes to address data protection risks after the design of a process or system has been finalised or implemented will likely lead to increased cost and effort. Some examples of when to conduct a DPIA include:

a) Creating a new system that involves the handling of personal data (e.g. new website that collects personal data);
b) Creating a new process, including manual processes, that involves the handling of personal data (e.g. receptionist collecting personal data from visitors);
c) Changing the way that existing systems or processes handle personal data (e.g. redesign of the customer registration process);
d) Changes to the organisational structure that affects the department handling personal data (e.g. mergers and acquisition, restructuring); and
e) Collecting new types of personal data (e.g. collecting new information about existing customers).

The significance of data protection risks can be evaluated based on their likelihood and impact. Defining risk criteria should include establishing specific criteria for each level of likelihood and impact, the scale of each, and risk acceptance criteria. Organizations should use a risk assessment framework that suits their objectives and needs. When defining risk criteria, organizations may consider legal and regulatory requirements, industry best practices or guidelines and project-specific requirements. Below is an example of a risk framework where data protection risks are assessed by multiplying projected or estimated likelihood and impact levels to obtain a quantitative risk rating. Each criterion is based on a five-point scale. This means that "1" is the lowest possible risk rating and "25" is the highest possible risk rating. The risk acceptance criterion is set at "15" and data protection risks with a risk rating of "15" and above will be given immediate priority. Here is an example of a data protection risk which is divided into likelihood criteria and impact criteria.:

a) **Likelihood Criterian**
   1. **Rare**, Remote and not conceivable;
   2. **Unlikely**, Conceivable but no indications or evidence to suggest possibility of occurrence in the near term;
   3. **Possible**, Indications suggest possibility of occurrence in the near term;
   4. **Likely**, Indications suggest expected occurrence in the near term; and
   5. **Almost Certain**, Indications suggest high probability of occurrence in the near term.

b) **Impact Criterian**
   1. **Insignificant**, remote and no impact;
   2. **Minor**, May experience inconvenience, but no indications or evidence to suggest major damage which will result in financial/ reputation loss;

3. **Moderate**, Experience some inconvenience or consequences, though indications suggest damage can be overcome or recovered in a short time;
4. **Major**, Experience significant consequences, with indications suggesting damage will be widespread, resulting in financial/reputation loss, and loss of support from stakeholders; and
5. **Severe**, Experience severe consequences, with indications suggesting that damage sustained may prevent organisation from operating as usual for a prolonged period of time, or which they may not be able to overcome.

Under Singapore's personal data protection rules, while there is no separate obligation to conduct a DPIA under the PDPA, there are provisions in the PDPA that require organizations to conduct an 'assessment' (which may be narrower in scope than a full DPIA) in certain circumstances. The PDPA covers personal data stored in electronic and non-electronic formats. It generally does not apply to: Any individual acting on a personal or domestic basis. Any individual acting in his/her capacity as an employee with an organisation. Any public agency in relation to the collection, use or disclosure of personal data. Business contact information such as an individual's name, position or title, business telephone number, business address, business email, business fax number and similar information.

Specifically, the obligation to conduct certain assessments under the PDPA rests with the organization (Section 15A(4)(a) and Paragraph 1(2)(a), Part 3 of the PDPA First Schedule). In addition, the PDPC recommends that

DPIAs be conducted, as part of an organization's 'Data Protection Management Program' and their obligation to develop and implement the policies and practices necessary for the organization to comply with the PDPA (Page 5 of the DPIA Guidelines and Pages 12 to 13 of the Management Program Guidelines). Specifically, the conduct of a DPIA should be led by, among others, the project manager or project focal point and DPO, as well as senior management within an organization (Page 8 of the DPIA Guidelines).[38]

The provisions Section 56 PDPA are a penalty for an individual violating personal data protection in cases where the punishment is not explicitly regulated in Sections of the PDPA. The additional fine for ongoing offences after conviction clarifies Singapore Government's staunch commitment to personal data protection. This provision indicates that all offenses will still receive a commensurate penalty even if not explicitly regulated in Sections of the PDPA. Section 56 of the PDPA regulates that:

> "*A person guilty of an offence under this Act for which no penalty is expressly provided shall be liable on conviction to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 3 years or to both and, in the case of a continuing offence, to a further fine not exceeding $1,000 for every day or part of a day during which the offence continues after conviction.*"

[38] K. C. Lim (2023). Singapore - Data Protection Overview. DataGuidance.Com. https://www.dataguidance.com/notes/singapore-data-protection-overview#:~:text=26%20of%202012)%20('PDPA,that%20a%20reasonable%20person%20would

IV. Conclusion

Based on the results of the analysis above, it can be seen that Data Protection Impact Assessment is an effort to approach risk management of personal data belonging to personal data subjects through consideration of its nature, scope, context, and purpose, likely to cause high risks to individual rights and freedoms. In the Indonesian legal space, Data Protection Impact Assessment is implicitly explained in Article 34 paragraph (1) of Law Number 27 Year 2022 on Personal Data Protection which is then further regulated through a Government Regulation as mandated by Article 34 paragraph (3). However, the Government Regulation relating to this matter has not yet been ratified. So there is no mandate that explicitly explains the indicators for the execution of Data Protection Impact Assessment in Indonesia. However, in this case, there are several mandates in the body of Law Number 27 of 2022 that can be used as a backup and need to be considered for the execution of Data Protection Impact Assessment, namely the mandate of Article 16 paragraph (2), Article 34 paragraph (1) and (2), Article 35, Article 20 paragraph (2), and Article 27 of Law Number 27 of 2022. Protection of consumer personal data on e-commerce platforms when viewed from the rights of personal data subjects based on Law Number 27 of 2022, things that need to be considered are the rights of these personal data subjects mandated in Article 6 through Article 13 of Law Number 27 of 2022 with exceptions based on Article 15. For comparison, personal data protection indicators in Singapore includes identifying the personal data handled by the system or process, as well as the reasons for collecting the personal data, Identifying how the personal data flows through the system or process, Identifying data protection risks by analysing the personal data handled and its data flows against requirements or data protection best practices, Addressing the identified risks by amending the system or process design, or introducing new organisation policies, Checking to ensure that identified risks are adequately addressed before the system or process is in effect or implemented.

V. References

Afifah, Yuni. "Pakar Hukum Siber UNAIR Jelaskan Prinsip Perlindungan Data Pribadi." fh.unair.ac.id, 2023. https://fh.unair.ac.id/pakar-hukum-siber-unair-jelaskan-prinsip-perlindungan-data-pribadi/.

Agung, Sagdiyah Fitri Andani Tambunan, and Muhammad Irwan Padli Nasution. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Di E-Commerce." *Jurnal Ekonomi Manajemen Dan Bisnis (JEMB)* 2, no. 1 (2023): 5–7. https://doi.org/10.47233/jemb.v2i1.915.

Al, Rifqy, Muh, Hidayatullah Arham, and M Chaerul Risal. "PERLINDUNGAN DATA PRIBADI BAGI

PENGGUNA MEDIA SOSIAL." *Jurnal Al Tasyri'iyyah* 3, no. 2 (2023): 109–19.

Bahtiar, Rais Agil. "Potensi, Peran Pemerintah, Dan Tantangan Dalam Pengembangan E-Commerce Di Indonesia [Potency, Government Role, and Challenges of E-Commerce Development in Indonesia]." *Jurnal Ekonomi Dan Kebijakan Publik* 11, no. 1 (2020): 13–25. https://doi.org/10.22212/jekp.v11i1.1485.

Budhijanto, Danrivanto. *Hukum Telekomunikasi, Penyiaran & Teknologi Informasi: Regulasi & Konvergensi*. Bandung: PT. Refika Aditama, 2010.

Corte, Dalla, Lorenzo, Van Brakel, and Rosamunde. "Data Protection Impact Assessment Methods for The Urban Environment." Tilburg, 2022.

Culnan, Mary J., and Robert J. Bies. "Consumer Privacy: Balancing Economic and Justice Considerations." *Journal of Social Issues* 59, no. 2 (2003): 323–42.

Dhaka, S. S. "Impact Od Growing E-Commerce on Indian Farmers." *Indian Journal of Economics and Development* 13, no. 2 (2017): 596.

Disemadi, Hari Sutra. "Urgensi Regulasi Khusus Dan Pemanfaatan Artificial Intelligence Dalam Mewujudkan Perlindungan Data Pribadi Di Indonesia." *Jurnal Wawasan Yuridika* 5, no. 2 (2021): 177. https://doi.org/10.25072/jwy.v5i2.460.

Garfinkel, S. *Database Nation: The Death of Privacy in the 21st Century*. California: O'Reilly Media, Inc, 2000.

Gellman, Robert. "Willis Ware's Lasting Contribution to Privacy: Fair Information Practices." *IEEE Security & Privacy* 12, no. 4 (2014): 51–54.

Halim, Etania Fajarani. "Perlindungan Hukum Data Pribadi

Pembeli Di Perdagangan Secara Elektronik (E-Commerce) Di Indonesia." *Jurnal Hukum Visio Justisia* 2, no. 1 (2022): 1–22. https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_233321.aspx.

Ibrahim, Jhony. *Teori Dan Metodologi Penelitian Hukum Empiris*. Malang: Bayumedia Publishing, 2006.

Ilm, Muhammad Irfan, Geger Jaka Kiswara, and Syarif Mustika. "PERLINDUNGAN DATA PRIBADI PENGGUNA APLIKASI PADA SMARTPHONE DITINJAU DARI HUKUM POSITIF." *Nusantara: Jurnal Ilmu Pengetahuan Sosial* 9, no. 4 (2022): 2291–2303.

Kun, Eyup. "Exploring the Role of Data Protection Impact Assessments in the Use of Facial Recognition Technologies: From Accountability to Meta-Regulation." *Social Science Research Network*, 2022. https://dx.doi.org/10.2139/ssrn.4239404.

Lim, C. K. (2023). Singapore - Data Protection Overview. DataGuidance.Com.https://www.dataguidance.com/notes/singapore-data-protection-overview#:~:text=26 of 2012) ('PDPA,that a reasonable person would.

Nafiah, R. "Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce." *Cyber Security Dan Forensik Digital* 3, no. 1 (2020): 18.

Niffari, Hanifan. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif Dengan Peraturan Perundang-Undangan Di Negara Lain)." *Jurnal Yuridis* 7, no. 1 (2020): 105–119. https://doi.org/10.35814/selisik.v6i1.1699.

Pahlevi, Reza. “Nilai Transaksi E-Commerce Indonesia Diperkirakan Capai US$137,5 Miliar Pada 2025.” Databoks.katadata.co.id, 2022. https://databoks.katadata.co.id/datapublish/2022/03/18/nilai-transaksi-e-commerce-indonesia-diperkirakan-capai-us1375-miliar-pada-2025.

Patnistik, Egidius. “Hak-Hak Setiap Subyek Data Pribadi Yang Perlu Dipahami.” Kompas.com, 2022. https://www.kompas.com/tren/read/2022/12/20/110721965/hak-hak-setiap-subyek-data-pribadi-yang-perlu-dipahami?page=all.

Perwitasari, Anna Suci. “Google CS Ungkap Alasan Potensi Perlambatan Pertumbuhan Penjualan E-Commerce.” Kontan.co.id2, 2023.

Pohan, Tia Deja, and Muhammad Irwan Padli Nasution. “PERLINDUNGAN HUKUM DATA PRIBADI KONSUMEN DALAM PLATFORM E COMMERCE Tia.” *SAMMAJIVA: Jurnal Penelitian Bisnis Dan Manajemen* 1, no. 3 (2023): 42–48. https://doi.org/10.32505/jurisprudensi.v15i1.5478.

Priscyllia, Fanny. “Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum.” *Jatiswara* 34, no. 3 (2019): 239–249.

Publication Team. “Special Categories of Personal Data - GDPR EU.” GDPR.EU.org, 2020. https://www.gdpreu.org/the-regulation/key-concepts/special-categories-personal-data/.

Putra, Tegar Islami. “The Analysis of the Legal Protection of Ship’s Crew in Sea Work Agreement in Indonesia.” *Indonesian Journal of Advocacy and Legal Services 5*, no.

2, (2023): 181–206. https://doi.org/10.15294/ijals.v5i2.75367.

Ramadhani, Syafira Agata. “Komparasi Perlindungan Data Pribadi Di Indonesia Dan Uni Eropa.” *Jurnal Hukum Lex Generalis* 3, no. 1 (2022): 73–84. https://doi.org/10.56370/jhlg.v3i1.173.

Rukmayuninda Ririh, Kirana, Nur Laili, Adityo Wicaksono, and Silmi Tsurayya. “Penggunaan Data Kesehatan Pribadi Dalam Era Big Data: Tantangan Hukum Dan Kebijakan Di Indonesia.” *Journal Ners* 15, no. 2 (2020): 864–70. http://journal.universitaspahlawan.ac.id/index.php/ners/article/view/16088.

Rusmawati, Dianne Eka. “Perlindungan Hukum Bagi Konsumen Dalam Transaksi E-Commerce.” *At Justisia Jurnal Ilmu Hukum* 7, no. 2 (2013): 195–97.

Sangojoyo, Bram Freedrik, Aurelius Kevin, and David Brilian Sunlaydi. “Urgensi Pembaharuan Hukum Mengenai Perlindungan Data Pribadi E-Commerce Di Indonesia.” *Kosmik Hukum* 22, no. 1 (2022): 27. https://doi.org/10.30595/kosmikhukum.v22i1.12154.

Soekanto, Soerjono, and Sri Mamudji. *Penelitian Hukum Normatif Tinjauan Singkat*. Jakarta: Rajawali Press, 2006.

Sulistianingsih, Dewi, Miftakhul Ihwan, Andry Setiawan, and Muchammad Shidqon Prabowo. “Tata Kelola Perlindungan Data Pribadi Di Era Metaverse (Telaah Yuridis Undang-Undang Perlindungan Data Pribadi).” *Masalah-Masalah Hukum* 52, no. 1 (2023): 97–106. https://doi.org/10.14710/mmh.52.1.2023.97-106.

Suparni, Niniek. *Cyberspace Problematika & Antisipasi*

Pengaturannya. Jakarta: Sinar Garfika, 2009.

Suyatno. "Analisa Perlindungan Data Pribadi Pengguna Fintech Berdasarkan Pendekatan Yuridis Normatif Di Indonesia." *YUME: Journal of Management* 5, no. 3 (2022): 481–91. https://doi.org/10.37531/yume.vxix.325.

Tim Publikasi. "FGD Tentang Data Protection Impact Assessment (DPIA) Dalam Pemrosesan Data Biometrik." Atmajaya.ac.id, 2023. https://www.atmajaya.ac.id/id/pages/fgd-dpia-lppm/.

Wahyuni, Willa. "Melihat Prinsip Dan Dasar Pemrosesan Data Pribadi." hukumonline.com, 2023. https://www.hukumonline.com/berita/a/melihat-prinsip-dan-dasar-pemrosesan-data-pribadi-lt64a2df2ad70ce/?page=2.

Yudistira, Muhammad, and Ramadhan. "Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 Oleh Kominfo." *Unes Law Review* 5, no. 4 (2023): 3802–15. https://doi.org/10.31933/unesrev.v5i4.

Acknowledgment

None

Funding Information

None

Conflicting Interest Statement

There is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Ei incumbit probatio quidicit,

nonqui negat