Journal of Private and Commercial Law

A peer-reviewed journal published by Faculty of Law Universitas Negeri Semarang, Indonesia. The title has been indexed by DOAJ, SINTA, GARUDA. ISSN 2599-0314 (Print) 2599-0306 (Online)
Online at https://journal.unnes.ac.id/journals/index.php/jpcl/index

Liability of E-Commerce Service Providers for Processing Consumer Personal Data (Comparative Study of Indonesia & Europe)

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

Nurul Fibrianti
Universitas Negeri Semarang, Indonesia
nurulfibrianti@mail.unnes.ac.id

Rizky Andeza Prasetya
University of Technology Malaysia
rizky@graduate.utm.my

Abstract

This study examines the regulatory mandate governing the liability of E-Commerce service providers in protecting personal data in personal data processing according to Law Number 27 of 2022 and General Data Protection Regulation. To support the fulfilment of the rights of consumers as owners of personal data and E-Commerce service providers as controllers of personal data, it is necessary to study the regulation of the liability of E-Commerce service providers in protecting personal data in personal data processing in other countries that first have personal data protection arrangements. The research method used to achieve the research objectives and targets is normative legal research with a legislative and comparative approach. The type of research used in this research is normative juridical research that gathers primary data through the analysis of relevant legal regulations and also includes the use of supporting scholarly journals. E-Commerce Service Providers as Personal Data Managers Against Consumer Personal Data Processing in Europe, in principle, have the same form of personal data processing as Indonesia, namely processing of personal financial data, full name, gender, nationality, user location, and personal data combined to identify a person in the form of telephone numbers and IP Addresses. However, European countries have different types of personal data from the rules in Indonesia.

KEYWORDS: ***Liability; E-Commerce Service; Processing; Consumer Personal Data***

Introduction

The rapid development of telecommunications technology and computer technology has resulted in a multifunctional internet. The internet is a medium that is utilized for various activities, including browsing, surfing, searching for data and news, sending messages via email, and trading. The high needs of the world community make the internet always one of the choices for online shopping through e-commerce involving various parties.[1] E-commerce is a series of business activities involving consumers, producers, service providers, and trade intermediaries using computer networks. This business activity gives roles and responsibilities to each party, especially for service provider companies as an instrument that brings the parties together. In companies and trade, every party wants all practical and safe realizations, especially in payment traffic.[2] This is what initiated the presence of E-Commerce. E-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.[3] The development of E-Commerce is maneuvering so fast around the world that Indonesia is no exception. Based on RedSeer's analysis, Indonesia's e-commerce market is projected to increase to US$137.5 billion by 2025.[4] In it's utilization, E-Commerce offers various conveniences, speed and ease of access. The adoption of E-Commerce has the potential to speed up processes, save costs, and accelerate the exchange

[1] Didik Kusuma Yadi, Muhammad Sood, and Dwi Martini, "Perlindungan Hukum Bagi Para Pihak Dalam Transaksi E-Commerce Menurut Tata Hukum Indonesia," *Jurnal Commerce Law* 2, no. 1 (2022): 47.
[2] Tegar Islami Putra, "Juridical Analysis of The Application of Local Currency Settlement Between Indonesia and China in Business Transactions," *Journal of Private and Commercial Law* 7, no. 2 (2023): 24.
[3] Tegar Islami Putra, "Data Protection Impact Assessment Indicators In Protecting Consumer E-Commerce Platforms," *The Indonesian Journal of International Clinical Legal Education* 6, no. 1 (2024): 12.
[4] 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.

of goods. Individuals who wish to engage in commerce can easily select or review merchandise through a company's website.[5]

The juridical basis for the protection of personal data comes from Article 28G of the 1945 Constitution, the fourth amendment of which reads, "Everyone has the right to protection of self, family, honor, dignity and property under his/her control, and is entitled to a sense of security and protection from threats of fear to do or not do something is a basic right". Thus, the protection of personal data is one form of realization of the constitutional mandate and must be regulated in the form of laws. In this case, personal data must be maintained reliably and securely so that there is no failure of personal data protection in the E-commerce media.[6]

E-commerce is a business activity that involves consumers, manufacturers, service providers, and intermediary traders using computer networks, namely the internet.[7] In the implementation of E-Commerce, the party has potential personal data issues in its execution as E-Commerce is the manager of personal information and data. As this personal information may include customer names, addresses, contact details, bank account details, likes, clicks, reviews and more. Most companies use this information to recommend related products, improve customer service, advertise, and design other marketing techniques and strategies.[8] With the growing trend of e-commerce, threats, hacking, online fraud, and conflicting activities are

[5] Embun Febryanti Panggabean et al., "Perkembangan Teknologi E-Business Terhadap Globalisasi Modern Pada Saat Ini," *Jurnal Manajemen Dan Ekonomi Kreatif* 2, no. 1 (2024): 134.
[6] Maldi Omar Muhammad and Lucky Dafira Nugroho, "Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi," *Pamator Journal* 14, no. 2 (2021): 168.
[7] Mariam Darus Badrulzaman et al., *Kompilasi Hukum Perikatan* (Jakrata: Citra Aditya Bakti, 2001): 283.
[8] Moutaz Haddara, A. Salazar, and Marius Langseth, "Exploring the Impact of GDPR on Big Data Analytics Operations in the E-Commerce Industry," *Procedia Computer Science* 219, no. 2022 (2023): 769.

emerging along with the E-commerce trend.[9] This is no exception to the management of personal data as a juridically protected matter in Indonesia, which is more specialized after the issuance of Law Number 27 of 2022 concerning Personal Data Protection. Basically, by deciding to use e-Commerce, consumers are required to be willing to provide personal data that is confidential when registering and making transactions.[10]

The problem of personal data in the world cannot be underestimated. Globally, accounts that experienced data leaks until the third quarter of 2022 reached 72.45 million accounts.[11] As for Indonesia, there are quite a lot of data leaks by various parties. Such as the leak of BPJS personal data, the case of the leak of 18.5 million BPJS Employment user data sold on a dark forum for IDR 153 million, the leak of personal data belonging to Bank Syariah Indonesia reaching 1.5 TB, including 15 million user data and passwords for internal access and services and customer personal data as well as loan information, data on 34,900,867 Indonesian passports, and 337 million personal data belonging to the Directorate General of Population and Civil Registration of the Ministry of Home Affairs.[12]

In relation to personal data protection, one of the references for drafting personal data protection laws in various countries today is the European Union's General Data Protection Regulation (GDPR). The package of regulations passed by the European Union in 2016 has influenced a number

[9] Saloni Srivastava and Shobhna Jeet, "E-Commerce and Privacy Issues," *Russian Law Journal* XI, no. 5 (2023): 2171.
[10] L. P. G Profumo, "The Drivers of the Intention to Cruise during the Covid-19 Pandemic: The Role of the Willingness to Share Personal Information.," *Sinergie: Italian Journal of Managemen* 40, no. 1 (2022): 105.
[11] Cindy Mutia Annur, "Indonesia Masuk 3 Besar Negara Dengan Kasus Kebocoran Data Terbanyak Dunia," Katadata.co.id, 2022, https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia.
[12] Publication Team, "4 Kasus Kebocoran Data Di Semester I 2023, Mayoritas Dibantah," CNNIndonesia.com, 2023, https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah.

of personal data protection policies around the world.[13] Some of the principles and principles contained in the GDPR rules are the basis including, validity, fairness, transparency, limitation of purpose, data minimization, accuracy, integrity, confidentiality, data security and the creation of mutual obligations as "supervisors" of personal data, so that it can be understood by various groups for the common goal. The rules also include company obligations, consumer service rules and rules for storing consumers' personal data.[14] As a rule that serves as a foundation for personal data protection rules around the world, it is interesting to compare the responsibility of e-Commerce service providers for consumers' personal data between Indonesian and European regulations.

Studies on the comparison of Indonesian and European personal data regulations have been conducted, including research by Hakim in 2023 which conducted a legal comparison of personal data protection regulations between the European Union and Indonesia. This research aims to analyses whether the laws and regulations in Indonesia have provided protection regarding personal data and how the European Union and Indonesian laws compare in regulating personal data protection. The results of the research show that in the European Union there is a prohibition to disclose all information that reveals the identity of users, as described in article 9 of the GDPR and has not been explicitly regulated in Indonesia.[15]

Although these studies are generally related to legal issues, this research does not explain specifically and specifically about the comparison of the

[13] Normand Edwin Elnizar, "Ini 4 Perbedaan GDPR Dan Perlindungan Data Pribadi Di Indonesia," hukumonline.com, 2019, https://www.hukumonline.com/berita/a/ini-4-perbedaan-gdpr-dan-perlindungan-data-pribadi-di-indonesia-lt5d513741ccedd/#.

[14] Namrysilia Buti Anjawai, F. Yudhi Priyo Amboro, and Rufinus Hotmaulana Hutauruk, "Perbandingan Perlindungan Hukum Terkait Data Pribadi Di Indonesia Dan Jerman," *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam* 4, no. 2 (2022): 209.

[15] Guswan Hakim, Oheo Kaimuddin Haris, and Muthaharry Mohammad, "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa Dan Indonesia Comparative Analysis of Laws Concerning Personal Data Protection Regulations Between the European Union and Indonesia," *Halu Oleo Legal Research* | 5, no. 2 (2023): 447.

responsibility of E-Commerce service providers for consumer personal data between personal data protection arrangements in Indonesia and Europe. Therefore, this research proposal has a high level of novelty and can have a direct impact on the academic community in Indonesia. Based on the background described above, the researcher is interested in researching and analyzing the "Liability of E-Commerce Service Provider for Consumer Personal Data (Comparative Study of Indonesia & Europe)". This research raises two research questions: 1) What is the form of consumer personal data processing for the management of E-Commerce Platforms in Indonesia? 2) How is the Comparison of the Obligations of E-Commerce Service Providers for Processing Consumer Personal Data between Indonesia and the European Union?

Method

The research approach used in this study is normative juridical research by collecting primary data through analysis of relevant legal regulations and also includes the use of supporting scientific journals. Normative juridical research collects primary data through analysis of relevant legal regulations, ranging from laws to ministerial regulations, and also uses supporting scientific journals. In addition, secondary data is collected through interviews with relevant parties.[16]

Result and Discussions

Forms of Processing Consumer Personal Data on the Management of E-Commerce Platforms in Indonesia

In general, personal data consists of facts relating to an individual that constitute information so personal that the person concerned wishes to keep

[16] Irwansyah, *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel* (Yogyakarta: Mirra Buana Media, 2020): 49.

it to himself and/or restrict others from disseminating it to other parties or misusing it.[17] In particular, personal data describes information that is closely related to a person that will distinguish the characteristics of each individual.[18] The definition of Personal Data in Article 1 paragraph (1) of Law No. 27 of 2022 on Personal Data Protection explains that, "*Personal Data is data about an identified or identifiable individual individually or in combination with other information either directly or indirectly through electronic or non-electronic systems*". In the management of consumer personal data by E-Commerce Platforms, it does not have a different interpretation of this definition.

Article 4 paragraph (1) of Law No. 27 of 2022 divides 2 types of personal data, namely specific personal data and general personal data. This division of types of personal data is carried out to provide a nomenclature that 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.

Furthermore, Article 4 paragraph (2) provides details on the classification of specific personal data, namely health data and information, biometric data, genetic data, criminal records, child data, personal financial data, and/or other data in accordance with the provisions of laws and regulations. For general personal data, the details are explained in Article 4 paragraph (3). In the case of combined personal data, it is further explained in the Explanation of Article 4 paragraph (3) letter f, that personal data combined to identify a person include cellular telephone numbers and IP

[17] Taufik Hidayat Telaumbanua, Deasy Soeikromo, and Delasnova S. S. Lumintang, "Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut Hukum Positif," *Jurnal Fakultas Hukum Unsrat Lex Privatum* 13, no. 1 (2024): 5.
[18] Jerry Kang, "Information Privacy in Cyberspace Transaction," *Stanford Law Review* 50, no. 4 (1998): 5.

Address as general personal data.[19] This personal data is actually data that is classified as Personally Identifiable Information (PII). PII is information that, when used alone or with other relevant data, can identify a person.[20]

The types of personal data above also apply and are things that include consumer personal data that is protected in the management of E-Commerce applications. And also applies all the principles of the implementation of Law Number 27 of 2022 as explicitly explained in Article 3, that this Law is based on protection, legal certainty, public interest, expediency, prudence, balance, responsibility, and confidentiality. Processing of Consumer Personal Data on the Management of E-Commerce Platforms is a matter that categorizes the type of personal data and has an implementation basis as explained above. In every transaction both conventional and e-commerce will always utilize money. In this case, money as an object approved by the community as an intermediary tool for conducting exchange or trade.[21]

Financial management by e-commerce is basically a form of electronic money. In this case, electronic money has a juridical basis in Article 2 paragraph (5) of Government Regulation of the Republic of Indonesia Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions which explains that an Electronic System Operator that has a portal, website, or application in a network via the internet which is used to provide, manage, and/or operate financial transaction services is a Private Scope Electronic System Operator. The form of consumer financial management carried out by E-Commerce is a means of payment between

[19] Tegar Islami Putra, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman, "Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations," *Contemporary Issues on Interfaith Law & Society* 4, no. 1 (2024): 93.
[20] Ake Frankenfield, "What Is Personally Identifiable Information (PII)? Types and Examples," Investopedia.com, 2024, https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp.
[21] Santi Endriani, "Konsep Uang: Ekonomi Islam VS Ekonomi Konvensional," *Anterior Jurnal* 15, no. 1 (2015): 73.

sellers and buyers as in line with the mandate of Article 60 paragraph (1) of Government Regulation of the Republic of Indonesia Number 80 of 2019 concerning Trade Through Electronic Systems. It is further explained in Article 60 paragraph (3) that Payment through the Electronic System as referred to in paragraph can be made using banking system facilities or electronic payment systems. This is one of the impacts of information digitalization.[22]

Meanwhile, personal data in the form of full name, gender, nationality, and personal data combined to identify a person in the form of a telephone number is data that is managed and processed by E-Commerce to identify consumers and other users of the E-Commerce platform as an identity and included as a legal subject. E-Commerce parties in terms of managing their platforms must have, include, or convey the identity of clear legal subjects as mandated by Article 9 paragraph (1) of Government Regulation of the Republic of Indonesia Number 80 of 2019 concerning Trading Through Electronic Systems. Furthermore, the explanation of Article 9 paragraph (1) explains that the identity of the legal subject in question is all information that explains the existence and legality of the legal subject concerned, both individuals and legal entities, which are listed in, among others, Identity Cards, Business Licenses, Legal Entity Ratification Decree Numbers, Business Actor Identity Numbers provided by the Minister, bank account numbers, or cellular telephone numbers.

In addition to cellular phone numbers, Law Number 27 of 2022 also mandates IP Address as combined personal data. IP Address is a series of numbers that become the identity of the device and is connected to the internet or other network infrastructure that has a function so that every

[22] Tegar Islami Putra and Nurul Fibrianti, "Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoritical Studies," *Annual Review of Legal Studies* 1, no. 2 (2024): 182.

device that uses an internet connection can contact each other.[23] IP Address is used to identify and direct data traffic between devices in a computer network.[24] IP Addresses are used as addresses assigned to computer networks and network equipment that use the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol. TCP/IP is a group of protocols that regulate computer data communication on the internet.[25] Every computer connected to the internet must at least have an IP address on every device connected to the internet and the IP address itself must be unique because no other computer/server/network device can use the same IP address on the internet. An IP address version 4 (IPv4) is a string of binary numbers 32 bits long that is used to identify devices on the network. An IP address is a 32-bit number separated by a period every 8 bits. Usually in use, IP addresses are written in four decimal numbers, each separated by a period.[26] In the processing of personal data, Fair Information Practices (FIPs) are principles that need to be observed internationally. In a 1973 report, a US government advisory committee initially proposed and named FIPs as a set of principles to protect the privacy of personal data in data storage systems. The Secretary's Advisory Committee on Automated Personal Data Systems published a report titled Records, Computers and the Rights of Citizens.[27] Reporting from the official website of The Federal Privacy Council United States, it is explained that FIPs are a collection of widely accepted principles that agencies use when evaluating information systems, processes, programs, and activities that affect individual privacy. FIPs are not a requirement, but rather a matter that each agency should

[23] S Arifin, "Implementasi Monitoring Jaringan Menggunakan Raspberry Pi Dengan Memanfaatkan Protokol SMTP (Simple Mail Transfer Protocol)," *JATI: Jurnal Mahasiswa Teknik Informatika* 1, no. 1 (2017): 38.
[24] Putra, *Loc.Cit*. 100.
[25] Arifin Hasnul, *Kitab Suci Jaringan Komputer Dan Koneksi Internet* (Yogyakarta: Mediakom, 2011): 38.
[26] Edi Winarno and Ali Zaki, *Web Programming Dengan Visual Basic* (Jakarta: PT. Elex Media Komputindo, 2010): 61.
[27] Borgesius et al., "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework," *Berkeley Technology Law Journal* 30, no. 3 (2015): 2082.

apply in accordance with the agency's mission and privacy program requirements. The principles are as follows:[28]

a. ***Access and Amendment***

Institutions must provide individuals with appropriate access to Personally Identifiable Information (PII) and appropriate opportunities to correct or amend it.

b. ***Accountability***

Agencies should be responsible for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define roles and responsibilities with respect to Personally identifiable information for all employees and contractors, and should provide appropriate training to all employees and contractors who have access to PII.

c. ***Authority***

Institutions may only create, collect, use, process, store, maintain, disseminate, or disclose PII if they are authorized to do so, and must identify this authorization in the appropriate notice.

d. ***Minimization***

Institutions may only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to achieve a lawful purpose, and may only retain PII for as long as necessary to achieve that purpose.

e. ***Quality and Integrity***

Institutions must create, collect, use, process, store, maintain, disseminate, or disclose PII with the accuracy, relevance, timeliness,

[28] *Ibid*.

and completeness reasonably necessary to ensure fairness to individuals.

f. Individual Participation

Agencies should involve individuals in the process of using PII and to the extent practicable, seek individuals' consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures for receiving and handling complaints and inquiries related to individual privacy.

g. Purpose Specification and Use Limitation

Institutions must provide notice of the specific purposes for which PII is collected and may only use, process, store, maintain, disseminate, or disclose PII for the purposes described in such notice and consistent with the purposes for which the PII was collected, or as otherwise legally permitted.

h. Security

Institutions must establish administrative, technical, and physical safeguards to protect PII with respect to the risk and magnitude of harm that would result from illegal access, use, modification, loss, destruction, dissemination, or disclosure of PII.

i. Transparency

Institutions must be transparent about information policies and practices with respect to PII, and must provide clear and accessible notice regarding the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.

Comparison of the Obligations of E-Commerce Service Providers Toward the Processing of Consumer Personal Data between Indonesia and the European Union

a. Obligation of E-Commerce Service Providers as Personal Data Controller Toward the Processing of Consumer Personal Data in Indonesia According to the Personal Data Protection Law

Article 3 letter g of Law Number 27 Year 2022 explains the mandate that the implementation of this Law is based on accountability. The principle of responsibility in the explanation of this Article explains that all parties related to the processing and supervision of Personal Data act responsibly so as to ensure the balance of rights and obligations of the parties involved, including the Personal Data Subject. This of course also has applicability to E-Commerce management companies in Indonesia.

E-Commerce management companies in Indonesia have the status of Personal Data Controller as mandated by Article 1 point 4 of Law No. 27 of 2022, which gives the meaning of personal data controller as any person, public body, and international organization acting individually or jointly in determining the purpose and exercising control of personal data processing. henceforth, the party that will carry out personal data processing is the personal data processor, which is any person, public body, and international organization acting individually or jointly in carrying out personal data processing on behalf of the personal data controller.

Juridically, the controller of personal data has obligations that must be fulfilled as mandated in Chapter VI of Law No. 27 of 2022. These obligations held by the controller of personal data are regulated in a separate article in the law.

Table 1: The Juridical Basis for the Obligations of Personal Data Controllers in the Processing of Personal Data According to Law of Indonesia Number 27 of 2022

No	Forms of Obligations of Personal Data Controllers in the Processing of Personal Data	Juridical Foundation (Law No. 27 of 2022)
1	Personal Data Controllers shall conduct limited and specific, lawful and transparent processing of Personal Data.	Article 27
2	The Controller of Personal Data shall carry out the processing of Personal Data with the aim of Processing Personal Data.	Article 28
3	The Personal Data Controller shall ensure the accuracy, completeness, and consistency of Personal Data in accordance with the provisions of the applicable Regulations by conducting verification.	Article 29 Paragraph (1) and Paragraph (2)
4	The Personal Data Controller must update and/or correct errors and/or inaccuracies in the Personal Data no later than 3x24 hours after the Subjek Data Pribadi Controller receives a request for updating and/or correcting the Personal Data and the Personal Data must be notified by the Personal Data Controller to the Personal Data Subject.	Article 30 Paragraph (1) and (2)
5	The Personal Data Controller shall refuse the request for access to the amendment of Personal Data to the Personal Data Subject in the event that: (a) Endangering the security, physical health, or mental health of the Personal Data Subject and/or other persons; (b) Affects the disclosure of Personal Data of others; and	Article 33

	(c) Contrary to the interests of the incumbent and national security.	
6	The Personal Data Controller shall record all processing of Personal Data.	Article 31
7	Access to track records of Personal Data processing must be provided by the Personal Data Controller to the Personal Data Subject no later than 3 x 24 hours.	Article 32 Paragraph (1) & Paragraph (2)
8	The Personal Data Controller shall conduct a Personal Data Protection assessment in the processing of high-risk Personal Data which includes: (a) automated decision-making that has significant legal consequences or impacts on Personal Data Subjects; (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.	Article 34 Paragraph (1) dan Paragraph (2)
9	The Controller of Personal Data shall have a Basis for Processing Personal Data.	Article 20 Paragraph (1)
10	The Personal Data Controller shall protect and ensure the security of the Personal Data processed by: (a) Formulation and implementation of technical operational measures to protect Personal Data from	Article 35

	interference with the processing of Personal Data contrary to the provisions of laws and regulations; and (b) Determining the level of security of Personal Data by taking into account the nature and risks of the Personal Data that must be protected in the processing of Personal Data.	
11	The Personal Data Controller shall maintain the confidentiality of Personal Data.	Article 36
12	The Personal Data Controller shall supervise the parties involved in the processing of Personal Data under the control of the Personal Data Controller.	Article 37
13	The Controller of Personal Data shall protect Personal Data from unauthorized processing and shall be obliged to safeguard it.	Article 38 and Article 39
14	In the case of processing of Personal Data that requires the valid consent of the Personal Data Subject, the consent shall be in writing or recorded electronically or non-electronically provided that the consent: (a) can be clearly distinguished from other matters; (b) made in a format that is understandable and easily accessible; and (c) using simple and clear language.	Article 22 Paragraph (1) and Paragraph (4)
15	In the case of any processing of Personal Data carried out with the consent of the Personal Data Subject, prior to any change of information, the Personal Data Controller shall provide information regarding: (a) the legality of the processing of Personal Data;	Article 21 Paragraph (1) dan Paragraph (2)

	(b) the purposes for which the Personal Data are processed; (c) the type and relevance of the Personal Data to be processed; (d) the retention period of documents containing Personal Data; (e) details regarding the Information collected; (f) the period of processing of Personal Data; and (g) rights of the Personal Data Subject.	
16	Change of information on the change of information on the processing of Personal Data with the valid consent of the Personal Data Subject as stated in Article 21 Paragraph 1, the Personal Data Controller shall notify the Personal Data Subject prior to the change of information.	Article 21 Paragraph (2)
17	For any processing of personal data carried out by a Personal Data Controller, the Personal Data Controller is obliged to demonstrate the consent that has been given by the Personal Data Subject.	Article 24
18	In the event that the Personal Data Subject withdraws the consent to the processing of Personal Data, the Personal Data Controller shall be obliged to cease the processing of Personal Data. The cessation of processing of Personal Data shall be carried out no later than 3 x 24 (three times twenty-four) hours as from when the Personal Data Controller receives the request to withdraw consent to the processing of Personal Data.	Article 40 Paragraph (1) dan Paragraph (2)
19	In the event of a request for the postponement and restriction of the processing of Personal Data, the Personal Data Controller shall be obliged to carry out the postponement	Article 41 Paragraph (1)

	and restriction of the processing of Personal Data either partially or wholly no later than 3x24 hours from the time the request is received by the Personal Data controller and the Personal Data Controller shall notify the Personal Data Subject in the event that the postponement and restriction has been carried out.	
20	The Controller of Personal Data shall end the processing of Personal Data in the event that: (a) It has reached the retention period (b) The purpose of processing Personal Data has been achieved; or (c) There is a request by the Personal Data Subject.	Article 42 Paragraph (1)
21	The Personal Data Controller shall delete Personal Data in the event that: (a) The Personal Data is no longer necessary for achieving the purposes of processing the Personal Data; (b) The Personal Data Subject has withdrawn consent to the processing of Personal Data; (c) There is a request from the Personal Data Subject; or (d) The Personal Data was obtained and/or processed unlawfully.	Article 43 Paragraph (1)
22	Personal Data Controller shall destroy Personal Data so that it can no longer be used to identify Personal Data Subjects in the event that: (a) The retention period has expired and is authorized to be destroyed based on the archive retention schedule; (b) There is a request from the Personal Data Subject; (c) Not related to the settlement of the legal process of a case; and/or (d) Personal Data obtained and/or processed by unlawful means.	Article 44 Paragraph (1)

23	The Personal Data Controller shall notify the erasure and/or destruction of Personal Data to the Personal Data Subject.	Article 45
24	In the event of a failure of Personal Data Protection, the Personal Data Controller shall notify in writing no later than 3 x 24 (three times twenty four) hours to the Personal Data Subject and the institution with the minimum substance of the notification containing: (a) Personal data disclosed; (b) When and how the Personal Data was disclosed; and (c) Handling and recovery efforts for the disclosure of Personal Data by the Personal Data Controller.	Article 46 Paragraph (1) dan Paragraph (2)
25	In the event of a failure of Personal Data Protection that disrupts public services and/or has a serious impact on public interests, the Personal Data Controller shall notify the public.	Article 46 Paragraph (3)

b. Liability of E-Commerce Service Providers as Personal Data Managers towards the Processing of Consumer Personal Data in Europe According to the General Data Protection Regulation of the European Union

Bacivally, the rules regarding Personal Data Processing in Indonesia and Europe do not have significant differences. The rules regarding the processing of Personal Data in the Europe Union General Data Protection Regulation (GDPR) are bound in different Articles and paragraphs depending on the classification of the mandate. The GDPR is the toughest privacy and security law in the world. Though it was drafted and passed by the European Union (EU), it imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU. The regulation was put into effect on May 25, 2018.

Table 2: The Juridical Basis for the Obligations of Personal Data Controllers in the Processing of Personal Data Under the General Data Protection Regulation

No	Forms of Obligations of Personal Data Controllers in the Processing of Personal Data	Juridical Foundation (General Data Protection Regulation)
1	The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.	Article 12 Paragraph 1
2	The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. In the cases referred to in Article 11(2), the controller shall not refuse to act on the request of the data subject for exercising his or her rights under Articles 15 to 22, unless the controller demonstrates that it is not in a position to identify the data subject.	Article 12 Paragraph 2
3	The controller shall provide information on action taken on a request under Articles 15 to 22 to the data subject without undue delay and in any event within one month of receipt of the request. 2That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. 3The controller shall inform the data subject of any such extension within one month of receipt of the request, together	Article 12 Paragraph 3

	with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.	
4	If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.	Article 12 Paragraph 4
5	Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of Article 6 (1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organization and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to	Article 13 Paragraph 1

	obtain a copy of them or where they have been made available.	
6	At the time when personal data are obtained, the controller shall provide the data subject with the following further information necessary to ensure fair and transparent processing: (a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability; (c) where the processing is based on point (a) of Article 6 Paragraph (1) or point (a) of Article 9 Paragraph (2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (d) the right to lodge a complaint with a supervisory authority; (e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data; (f) the existence of automated decision-making, including profiling, referred to in Article 22 Paragraph (1) and Paragraph (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	Article 13 Paragraph 2

7	Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in Paragraph 2.	Article 13 Paragraph 3
8	Where personal data have not been obtained from the data subject, the controller shall provide the data subject with the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller's representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) the categories of personal data concerned; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, that the controller intends to transfer personal data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.	Article 14 Paragraph 1
9	In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:	Article 14 Paragraph 2

	(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period; (b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party; (c) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability; (d) where processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; (e) the right to lodge a complaint with a supervisory authority; (f) from which source the personal data originate, and if applicable, whether it came from publicly accessible sources; (g) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.	
10	The controller shall provide the information referred to in paragraphs 1 and 2: (a) within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed; (b) if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or	Article 14 Paragraph 3

	(c) if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.	
11	Where the controller intends to further process the personal data for a purpose other than that for which the personal data were obtained, the controller shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in Paragraph 2.	Article 14 Paragraph 4
12	The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.	Article 15 Paragraph 3
13	The controller shall communicate any rectification or erasure of personal data or restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.	Article 19
14	The controller shall inform the data subject about those recipients if the data subject requests it.	Article 19
15	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to	Article 32 Paragraph 1

	the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.	
16	The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.	Article 32 Paragraph 4
17	In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.	Article 33 Paragraph 1
18	The notification referred to in paragraph 1 shall at least: (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the	Article 33 Paragraph 3

	categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned; (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; (c) describe the likely consequences of the personal data breach; (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.	
19	The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. 2That documentation shall enable the supervisory authority to verify compliance with this Article.	Article 33 Paragraph 5
20	When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.	Article 34 Paragraph 1
21	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.	Article 35 Paragraph 1

22	The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.	Article 35 Paragraph 2
23	The assessment shall contain at least: (a) systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; (d) and the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.	Article 35 Paragraph 7
24	Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.	Article 35 Paragraph 11
25	The controller shall consult the supervisory authority prior to processing where a data protection impact assessment under Article 35 indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.	Article 36 Paragraph 1
26	When consulting the supervisory authority pursuant to paragraph 1, the controller shall provide the supervisory authority with:	Article 36 Paragraph 3

(a) where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;
(b) the purposes and means of the intended processing;
(c) the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to this Regulation;
(d) where applicable, the contact details of the data protection officer;
(e) the data protection impact assessment provided for in Article 35; and
(f) any other information requested by the supervisory authority

*c. **Liability Comparison of E-Commerce Service Providers as Personal Data Controller towards the Processing of Consumer Personal Data According to the General Data Protection Regulation of the European Union and Indonesian Personal Data Protection Regulation***

Table 3: The Comparison of Juridical Basis for the Obligations of Personal Data Controllers in the Processing of Personal Data According to Law of Indonesia Number 27 of 2022 & Europe Union General Data Protection Regulation

No.	Form of Obligation	Law No. 27 of 2022 (Indonesia)	GDPR (Eropean Union)
1	Limited, specific, lawful & transparent processing	Article 27	Article 12(1)
2	Clear processing objectives	Article 28	Article 13(1)(c)
3	Data accuracy and verification	Article 29(1)-(2)	Article 16
4	Data update/correction	Article 30(1)-(2)	Article 12(3)

No.	Form of Obligation	Law No. 27 of 2022 (Indonesia)	GDPR (Eropean Union)
5	Denial of request that is harmful	Article 33	Article 23
6	Recording of all processing activities	Article 31	Article 30
7	Access to data processing history	Article 32	Article 15
8	Data Protection impact Assessment (DPIA)	Article 34	Article 35
9	Processing Basis	Article 20(1)	Article 6
10	Protect technically & operationally	Article 35	Article 32
11	Maintaining the confidentiality of personal data	Article 36	Article 5(1)(f)
12	Supervise parties involved in processing	Article 37	Article 28(1)
13	Prevention of unauthorized processing	Article 38–39	Article 32(4)
14	Valid & clear consent	Article 22(1)	Article 7
15	Information before processing	Article 21(1)	Article 13(2)
16	Notification of changes to information	Article 21(2)	Article 13(3)
17	Evidence of consent	Article 24	Article 7(1)
18	Termination after revocation of consent	Article 40(1)-(2)	Article 7(3)
19	Restriction/termination upon request	Article 41(1)	Article 18
20	Termination of processing when the purpose is achieved	Article 42(1)	Article 17(1)(a)
21	Data deletion	Article 43(1)	Article 17
22	Destruction of data to prevent identification	Article 44(1)	Article 17(2)

No.	Form of Obligation	Law No. 27 of 2022 (Indonesia)	GDPR (Eropean Union)
23	Notification of deletion/destruction	Article 45	Article 19
24	Leak notification to subjects and authorities	Article 46(1)-(2)	Article 33 (72 jam)
25	Public notification if serious impact	Article 46(3)	Article 34(1)

Based on the comparative analysis in Table 3, it can be seen that in general, Indonesian Law Number 27 of 2022 has similarities with the European Union General Data Protection Regulation in terms of Obligations of Personal Data Controllers in the Processing of Personal Data. However, there are differences in terms of Obligations that are regulated in Law Number 27 of 2022, but are implicitly explained in the European Union General Data Protection Regulation or even not regulated at all.

The first difference in Obligations of Personal Data Controllers in the Processing of Personal Data According to Law of Indonesia Number 27 of 2022 & European Union General Data Protection Regulation is with regard to the obligation to have a basis for processing. In Indonesia's PDP Law this is explicitly declared in Article 20 paragraph (1) whereas in the EU GDPR it is not explicitly declared. However, with regard to Article 6(1) of the EU GDPR. The GDPR does require the existence of a legal basis as an element of lawfulness of processing, but does not declaratively state an explicit obligation for controllers to establish a legal basis, in contrast to the approach of Indonesia's PDP Law which clearly mandates it. In addition, Indonesia's PDP Law declaratively stipulates the obligation to maintain the confidentiality of personal data. Whereas in the EU GDPR it becomes part of Article 5 Paragraph (1) (f).

Within the framework of the European Union's General Data Protection Regulation (GDPR), the obligation of a data controller to supervise other parties involved in data processing is not explicitly regulated in a single article as stipulated in Article 37 of Law No. 27 of 2022. However, similar principles and obligations are scattered in several provisions of the GDPR which functionally contain equivalent mandates. GDPR through Article 28 paragraph (1) states that the controller is only allowed to appoint data processors that provide sufficient guarantees in terms of technical and organizational protection of personal data. This provision is reinforced in Article 28 paragraph (3) GDPR which requires a written contract between the controller and the processor, specifying in detail that the processing is only carried out on the instructions of the controller, maintaining confidentiality, and implementing adequate technical protection measures. In addition, Article 32(4) of the GDPR extends the responsibilities of controllers and processors to internal personnel under their authority. This article requires controllers to ensure that any individual who has access to personal data can only perform processing in accordance with the controller's lawful instructions. Thus, the GDPR establishes a supervisory system through a contractual and instructional approach, where the controller is indirectly responsible through the control of internal processors and executors. Although not as explicit as the Law No. 27 of 2022 in its normative wording, the principles of responsibility and supervision attached to data controllers in the GDPR are similar in substance and provide a strong legal basis for the controller's accountability mechanism for the entire set of data processing under its control.

Conclusion

The study concludes that consumer personal data processing by e-commerce service providers in Indonesia, regulated under Law No. 27 of 2022 on Personal Data Protection, involves managing financial data, full name, gender, nationality, phone numbers, user location, and IP addresses. This data is used for payment transactions and user identification, with e-commerce platforms acting as personal data controllers responsible for ensuring security, accuracy, and confidentiality. When compared to the European Union's GDPR, both regulations share similar principles in protecting personal data. However, the GDPR provides broader protections by including genetic, physiological, mental, and social identity information. It also imposes stricter obligations, such as mandatory data protection impact assessments and transparency requirements. Although Indonesia's regulations align with global standards, further improvements are needed to enhance comprehensive personal data protection and meet the level of consumer data security outlined in the GDPR.

References

Anjawai, Namrysilia Buti, F. Yudhi Priyo Amboro, and Rufinus Hotmaulana Hutauruk. "Perbandingan Perlindungan Hukum Terkait Data Pribadi Di Indonesia Dan Jerman." *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam* 4, no. 2 (2022): 207–18. https://doi.org/10.37680/almanhaj.v4i2.1791.

Annur, Cindy Mutia. "Indonesia Masuk 3 Besar Negara Dengan Kasus Kebocoran Data Terbanyak Dunia." Katadata.co.id, 2022. https://databoks.katadata.co.id/datapublish/2022/09/13/indonesia-masuk-3-besar-negara-dengan-kasus-kebocoran-data-terbanyak-dunia.

Arifin, S. "Implementasi Monitoring Jaringan Menggunakan Raspberry Pi Dengan Memanfaatkan Protokol SMTP (Simple Mail Transfer Protocol)." *JATI: Jurnal Mahasiswa Teknik Informatika* 1, no. 1 (2017): 37–44.

Badrulzaman, Mariam Darus, Sutan Remy Sjahdeini, Heru Soepraptomo, Faturrahman Djamil, and Taryana Soenandar. *Kompilasi Hukum Perikatan*. Jakrata: Citra Aditya Bakti, 2001.

Bitrián, Paula, et al. "Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours." *Journal of Business Research* 179 (2024): 114685.

Borgesius, Frederik Zuiderveen, Jonathan Gray, and Mireille van Eechoud. "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework." *Berkeley Technology Law Journal* 30, no. 3 (2015): 2073–2131. https://www.jstor.org/stable/26377585.

Crawford, Allison D., et al. "A reproductive justice investigation of utilizing digital interventions among underserved populations with criminal legal system supervision: Policy brief." *Nursing Outlook* 73.2 (2025): 102349.

Elnizar, Normand Edwin. "Ini 4 Perbedaan GDPR Dan Perlindungan Data Pribadi Di Indonesia." hukumonline.com, 2019. https://www.hukumonline.com/berita/a/ini-4-perbedaan-gdpr-dan-perlindungan-data-pribadi-di-indonesia-lt5d513741ccedd/#.

Endriani, Santi. "Konsep Uang: Ekonomi Islam VS Ekonomi Konvensional." *Anterior Jurnal* 15, no. 1 (2015): 70–75. https://doi.org/10.33084/anterior.v15i1.201.

Fibrianti, N., Dahlan, T. A., Anitasari, R. F., Paramita, N. D., & Putra, T. I. "Review of Child Consumer Protection in the Practice of Online Gambling Games Through the Gacha System." *The Indonesian Journal of International Clinical Legal Education 6*, no.3 (2024) 427-452 https://doi.org/doi.org/10.15294/ijicle.v6i3.13198

Finaka, Andrean W. "Perjalanan UU Perlindungan Data Pribadi." Indonesiabaik.id, 2016. https://indonesiabaik.id/infografis/perjalanan-uu-perlindungan-data-pribadi.

Firdhausya, Mahima Umaela, Muhammad Hilmi Naufal Aflah, Anisa Tussaleha, Tegar Islami Putra, and Eko Mukminto. "The Urgency of Limiting The Utilization of Consumer IP Addresses By Companies as Personal Data Objects in The Study of Positive Law in Indonesia." Law Research Review Quarterly 10, no. 2 (2024): 393-410.

Frankenfield, Ake. "What Is Personally Identifiable Information (PII)? Types and Examples." Investopedia.com, 2024. https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp.

Guamán, Danny S., David Rodriguez, Jose M. del Alamo, and Jose Such. "Automated GDPR Compliance Assessment for Cross-Border Personal Data Transfers in Android Applications." *Computers and Security* 130, no. C (2023): 1–16. https://doi.org/10.1016/j.cose.2023.103262.

Haddara, Moutaz, A. Salazar, and Marius Langseth. "Exploring the Impact

of GDPR on Big Data Analytics Operations in the E-Commerce Industry." *Procedia Computer Science* 219, no. 2022 (2023): 767–77. https://doi.org/10.1016/j.procs.2023.01.350.

Hakim, Guswan, Oheo Kaimuddin Haris, and Muthaharry Mohammad. "Analisis Perbandingan Hukum Mengenai Regulasi Perlindungan Data Pribadi Antara Uni Eropa Dan Indonesia Comparative Analysis of Laws Concerning Personal Data Protection Regulations Between the European Union and Indonesia." *Halu Oleo Legal Research* | 5, no. 2 (2023): 443–53. https://ojs.uajy.ac.id/index.php/jik/article/view/682.

Hamid, Supardi, and Mohammad Nurul Huda. "Mapping the landscape of government data breaches: A bibliometric analysis of literature from 2006 to 2023." *Social Sciences & Humanities Open* 11 (2025): 101234.

Hasnul, Arifin. *Kitab Suci Jaringan Komputer Dan Koneksi Internet*. Yogyakarta: Mediakom, 2011.

Irwansyah. *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Yogyakarta: Mirra Buana Media, 2020.

Joyce, Aaron, and Vahid Javidroozi. "Smart city development: Data sharing vs. data protection legislations." *Cities* 148 (2024): 104859.

Kang, Jerry. "Information Privacy in Cyberspace Transaction." *Stanford Law Review* 50, no. 4 (1998): 5.

Kathole, Atul B., Amit Sanjiv Mirge, and Avinash P. Jadhao. "Advancing electronic medical data protection through blockchain innovation." *Blockchain and Digital Twin for Smart Hospitals*. Elsevier, 2025. 193-205.

Kun, Eyup. "Searching for the appropriate legal basis for personal data processing for cybersecurity purposes under the NIS 2 Directive: Legal obligation and/or legitimate interest?." *Computer Law & Security Review* 56 (2025): 106098.

Laurent, Maryline, and Claire Levallois-Barth. "Privacy Management and Protection of Personal Data." In *Digital Identity Management*, 137–205. Elsevier, 2015. https://doi.org/10.1016/B978-1-78548-004-1.50004-3.

Lim, Abigail Chiu Mei, Lynnette Hui Xian Ng, and Araz Taeihagh. "Biometric data landscape in Southeast Asia: Challenges and opportunities for effective regulation." *Computer Law & Security Review* 56 (2025): 106095.

Medina, Ayman Falak. "Indonesia's Personal Data Protection Law: Key Compliance Requirements." Aseanbriefing.com, 2022. https://www.aseanbriefing.com/news/indonesia-enacts-first-

personal-data-protection-law-key-compliance-requirements/.

Muh.Ikram, Idrus, and Nur Miftahul Janah. “Peranan Pasar Tradisional Dalam Meningkatkan Kesejahteraan Masyarakat (Studi Kasus Pada Pasar Pa’baeng-Baeng Di Kecamatan Tamalate Kota Makasar).” *Jurnal Ekonomi Balance Fakultas Ekonomi Dan Bisnis* 12, no. 2 (2016): 2.

Muhammad, Maldi Omar, and Lucky Dafira Nugroho. “Perlindungan Hukum Terhadap Pengguna Aplikasi E-Commerce Yang Terdampak Kebocoran Data Pribadi.” *Pamator Journal* 14, no. 2 (2021): 165–74. https://doi.org/10.21107/pamator.v14i2.12472.

Muin, Indriani. “Perlindungan Data Pribadi Dalam Platform E-Commerce Guna Peningkatan Pembangunan Ekonomi Digital Indonesia.” *MJP Journal Law and Justice (MJPJLJ)* 1, no. 2 (2023): 81–91. https://jurnalilmiah.co.id/index.php/MJPJLJ.

Novelli, Claudio, et al. "Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity." *Computer Law & Security Review* 55 (2024): 106066.

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.

Panggabean, Embun Febryanti, Hesty Ananta Yunas, Taufiqurrahman, and Nurbaiti. “Perkembangan Teknologi E-Business Terhadap Globalisasi Modern Pada Saat Ini.” *Jurnal Manajemen Dan Ekonomi Kreatif* 2, no. 1 (2024): 132–39. https://ukitoraja.id/index.php/jumek/article/view/284.

Profumo, L. P. G. “The Drivers of the Intention to Cruise during the Covid-19 Pandemic: The Role of the Willingness to Share Personal Information.” *Sinergie: Italian Journal of Managemen* 40, no. 1 (2022): 103–122.

Publication Team. “4 Kasus Kebocoran Data Di Semester I 2023, Mayoritas Dibantah.” CNNIndonesia.com, 2023. https://www.cnnindonesia.com/teknologi/20230720060802-192-975421/4-kasus-kebocoran-data-di-semester-i-2023-mayoritas-dibantah.

Putra, Tegar Islami. "*Analisis Yuridis Profesionalitas Pejabat Pelindungan Data Pribadi Dalam Melaksanakan Tugas Sesuai Undang-Undang Nomor 27 Tahun 2022"*. Semarang State University. 2025.

____. “Data Protection Impact Assessment Indicators in Protecting Consumer E-Commerce Platforms.” *The Indonesian Journal of International Clinical Legal Education* 6, no. 1 (2024): 1–22.

———. “Juridical Analysis of The Application of Local Currency Settlement Between Indonesia and China in Business Transactions.” *Journal of Private and Commercial Law* 7, no. 2 (2023): 13–34.

Putra, Tegar Islami, and Nurul Fibrianti. “Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoritical Studies.” *Annual Review of Legal Studies* 1, no. 2 (2024): 179–204.

_ _ _. (2024). "Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia." *Lambung Mangkurat Law Journal 9,* no. 1 (2024): 64–74. https://doi.org/10.32801/lamlaj.v9i1.438

Putra, T. I., Fibrianti, N., & Fakhrullah, M. R. (2025). Basis of Data Protection Officer Appointment : Comparative Study of Indonesia and European Union Regulation. *SASI*, *31*(1), 1–15. https://doi.org/10.47268/sasi.v31i1.2068.

Putra, T. I., Fibrianti, N., Fakhis, A. Z. P., & Fakhrullah, M. R. "Critically Reveal The Dimensions of Damage From Unauthorized Use of Personal Data." *The Digest: Journal of Jurisprudence and Legisprudence 5*, no.2 (2025) 231-262. https://doi.org/doi.org/10.15294/digest.v5i2.19941

Putra, Tegar Islami, Akbar Jihadul Islam, and Abdullah Mufti Abdul Rahman. “Integrating Islamic Laws into Indonesian Data Protection Laws: An Analysis of Regulatory Landscape and Ethical Considerations.” *Contemporary Issues on Interfaith Law & Society* 4, no. 1 (2024): 85–118.

Ramli, Ahmad M. *Cyber Law Dan HAKI Dalam Sistem Hukum Indonesia*. Jakarta: Refika Aditama, 2004.

Rawamangun Muka, Jl, Pulo Gadung, Kota Jakarta Timur, and Daerah Khusus. “Ethical Problems of Digitalization and Artificial Intelligence in Education: A Global Perspective.” *Journal of Pharmaceutical Negative Results* 14, no. 2 (2023): 2150–61. https://doi.org/10.47750/pnr.2023.14.S02.254.

Robles, Tomás, Borja Bordel, Ramón Alcarria, and Diego Sánchez-de-Rivera. “Enabling Trustworthy Personal Data Protection in EHealth and Well-Being Services through Privacy-by-Design.” *International Journal of Distributed Sensor Networks* 16, no. 5 (2020): 1-12. https://doi.org/10.1177/1550147720912110.

Srivastava, Saloni, and Shobhna Jeet. “E-Commerce and Privacy Issues.” *Russian Law Journal* XI, no. 5 (2023): 2170–75.

Telaumbanua, Taufik Hidayat, Deasy Soeikromo, and Delasnova S. S. Lumintang. “Perlindungan Hukum Bagi Pengguna Media Sosial Terhadap Penyalahgunaan Data Pribadi Terkait Hak Privasi Menurut

Hukum Positif." *Jurnal Fakultas Hukum Unsrat Lex Privatum* 13, no. 1 (2024): 5.

Waspiah, Waspiah, Noveria Sekar S, Ammirah Lies S, Tegar Islami Putra, Setyaning Wida N, and Salisa Widyaning K. "Model Pelindungan Hukum Data Pribadi Di Era Digital Guna Menjamin Hak Warga Negara Atas Pelindungan Data Pribadi." *Syntax Literate ; Jurnal Ilmiah Indonesia* 8, no. 9 (2023): 5165–79. https://doi.org/10.36418/syntax-literate.v8i9.13662.

Winarno, Edi, and Ali Zaki. *Web Programming Dengan Visual Basic*. Jakarta: PT. Elex Media Komputindo, 2010.

Xu, Shuo, et al. "FLPM: A property modification scheme for data protection in federated learning." *Future Generation Computer Systems* 154 (2024): 151-159.

Yadi, Didik Kusuma, Muhammad Sood, and Dwi Martini. "Perlindungan Hukum Bagi Para Pihak Dalam Transaksi E-Commerce Menurut Tata Hukum Indonesia." *Jurnal Commerce Law* 2, no. 1 (2022). https://doi.org/10.29303/commercelaw.v2i1.1368.

***

DECLARATION OF CONFLICTING INTERESTS

None.

FUNDING INFORMATION

None.

ACKNOWLEDGMENT

None.

HISTORY OF ARTICLE

Submitted : July 11, 2024
Revised : May 26, 2025
Accepted : May 30, 2025
Published : July 08, 2025