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

Risks of Consumer Personal Data Protection at the Personal Data Processing Stage of E-Commerce Websites

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

Adinda Zeranica Putri Fakhis
International Islamic University Malaysia, Malaysia
a.zeranicafakhis@student.iium.edu.my

Annisa Tussaleha
Universitas Negeri Semarang, Indonesia
annisatussaleha@student.unnes.ac.id

Mahima Umaela Firdhausya
Universitas Negeri Semarang, Indonesia
umaelafirdhausya@students.unnes.ac.id

Muhammad Hilmi Naufal Aflah
Unievrsitas Negeri Semarang, Indonesia
capasalfa065@students.unnes.ac.id

Abstract

The advancement of information and communication technology has made privacy boundaries thinner. Various personal data on E-Commerce websites are increasingly easy to spread, which creates risks at every stage of personal data processing. This is important to be given further attention, given the high number of transaction valuations that occur through E-Commerce websites. This research aims to analyze what forms of risks can occur at each stage of personal data processing on E-Commerce websites. The stages of personal data processing described in this research are the stages of personal data processing as stipulated in Article 16 Law Number 27 Year 2022 on Personal Data Protection. This research utilizes a library research method by focusing on legal materials so that it can be said to be library based. The results show that there are different risks at each stage of personal data processing on E-Commerce websites, both before the storage of personal data, and after the storage of personal data by the personal data controller. This can be in the form of

data collection that is not in accordance with applicable regulations, lack of transparency of data collection, and data collection that is not specific, unlimited, and illegal, unauthorized access, disclosure in an unauthorized manner, unauthorized modification, misuse, destruction, and loss of personal data on the system. To reduce the impact of risks, things that can be done are to update the system regularly, or increase the capacity of human resources who process personal data.

KEYWORDS: ***Risk; Consumer; Personal Data Processing; E-Commerce***

Introduction

E-Commerce is the process of trade transactions, be it goods, services, or information using the internet network.[1] 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[2]. 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). 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.[3] The rapid development of technology is one of the reasons for the rapid development of trade.[4] This was also triggered by internet infrastructure and mobile device penetration.[5] In addition, the increasing use of e-commerce is directly proportional to the threat of crime

[1] Tegar Islami Putra and Nurul Fibrianti, "Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoretical Studies: Kriminalisasi Konsumen Atas Kritik Yang Diberikan Kepada Perusahaan Melalui Dunia Maya Dalam Kajian Teoritis," *Annual Review of Legal Studies* 1, no. 2 (2024): 179–204.
[2] Khafidah Puspita, "Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia," *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan Dan Ekonomi Islam* 15, no. 2 (2023): 67–83.
[3] Reza Pahlevi, "Nilai Transaksi E-Commerce Indonesia Diperkirakan Capai US $137, 5 Miliar Pada 2025," *Databoks. Katadata. Co. Id*, 2022.
[4] Putra, Loc.Cit.
[5] Erna Priliasari, "Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 12, no. 2 (2023).

that comes with it.[6] Consumers face issues related to data privacy breaches, deceptive advertising, counterfeit products, and difficulties in resolving disputes.[7]

Personal data is one of the important issues in e-commerce. This is related to the confidentiality and protection of personal data.[8] Conducting and accepting online transactions, it is necessary to provide consumers' personal data.[9] In this research, it will make the mandate of Article 16 paragraph (1) of Law Number 27 of 2022 concerning Personal Data Protection as the processing flow studied. E-Commerce as the controller of personal data will later process the personal data. The processing of personal data by the personal data controller according to Article 16 paragraph (1) of Law No. 27 of 2022 on the Protection of Personal Data consists of obtaining and collecting, processing and analyzing, storing, repairing and updating, displaying, announcing, transferring, disseminating, or disclosing, as well as erasing or destroying. Each stage of processing has its own risks. Each stage of processing has its own risks. As another example of personal data, log data, which are considered input data for insider-threat detection technologies, encompasses a wide range of information from system activities to user interactions, and plays a pivotal role in cybersecurity.[10] This of course also applies to every stage of personal data processing carried out by e-commerce personal data controllers, both

[6] Topik Hidayat, Jeffry A Ch Likadja, and Petrus E Derozari, "PERLINDUNGAN HUKUM DATA PRIBADI KONSUMEN DALAM PERDAGANGAN ELEKTRONIK.," *Journal of Comprehensive Science (JCS)* 2, no. 5 (2023).
[7] Haris Satrio Dana et al., "Perlindungan Konsumen Dalam Perdagangan Elektronik (e-Commerce)," *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan| E-ISSN: XXXX-XXX* 1, no. 1 (2024): 82–86.
[8] Herdi Setiawan, Mohammad Ghufron, and Dewi Astutty Mochtar, "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce," *MLJ Merdeka Law Journal* 1, no. 2 (2020): 102–11.
[9] Tegar Islami Putra and Nurul Fibrianti, "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.
[10] Eyup Kun, "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.

before and after the storage of personal data. Given that the spread of information in the digital era of information and communication technology is currently so fast, global, and across national borders is a new challenge that causes an increased risk of privacy rights violations.[11] This research will analyze the risks of consumer personal data protection at the personal data processing stage of e-commerce websites. The urgency of this research is that it is hoped that all parties involved in personal data processing can find out what the risks of personal data processing are at each stage. Advances in information and communication technology have made privacy boundaries thinner. Various personal data are increasingly easy to spread.[12]

Similar research has been conducted by Putra entitled Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia published in Lambung Mangkurat Law Journal Volume 9 Issues 1 2023. The results showed that there are three forms of threats to people's personal data combined in e-commerce transactions, especially in the use of IP Addresses, namely the threat of geographic location tracking, unauthorized use and opening of personal data, and Distributed Denial of Service (DDoS) attacks.[13] However, The research object in this study is only limited to the combined Personal Data.

Other similar research has also been conducted by Dokuachev in his research entitled Classification of personal data security threats in information systems published in T-Comm-Телекоммуникации и Транспорт 14 (1) with the title Classification of personal data security threats in information systems. This research discusses the threats that arise when working with personal data in information systems. The results

[11] Fanny Priscyllia, "Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum," *Jatiswara* 34, no. 3 (2019): 239–49.
[12] Ririn Aswandi, Purti Rofifah Nabilah Muchin, and Muhammad Sultan, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)," *Jurnal Legislatif*, 2020, 167–90.
[13] Putra and Fibrianti, "Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia."

showed that some data are at risk in information systems, such as passport data, employment data, companies, contact details, telephone numbers, addresses, emails, and other information that represents an interest for potential computer attacks. The proposed classification can serve as the basis for threat models of certain information systems designed to process personal data.[14]

Other similar research has also been conducted by Spalevic in his research entitled GDPR and Challenges of Personal Data Protection published in The European Journal of Applied Economics. The results showed that the main premise of the development of the modern digital economy is based on the accelerated development of information and communication technology, while answering new challenges and threats to privacy and personal data protection. There are few number of potential risks: unauthorized disclosure, identity theft, or cyberbullying.[15]

Of all the studies that have been conducted as described above, none of the studies specifically discuss the Risk of Consumer Personal Data Protection at the Personal Data Processing Stage of E-Commerce Websites, especially in the process carried out before and after personal data storage is carried out. So this research has ~~a great~~ novelty value. This research provides an in-depth understanding of the risks faced by consumers regarding personal data protection at the data processing stage on e-commerce sites. This helps increase public and company awareness of the importance of maintaining consumer data privacy. Second, this research can serve as a foundation for the development of stronger policies and regulations to protect personal data in the e-commerce sector, both at the national and international levels. Third, this research offers practical recommendations for e-commerce managers in adopting technical and

[14] Vladimir A Dokuchaev, Victoria V Maklachkova, and V Yu Statev, "Classification of Personal Data Security Threats in Information Systems," *T-Comm-Телекоммуникации и Транспорт* 14, no. 1 (2020): 56–60.
[15] Kosana Vicentijevic, "GDPR AND CHALLENGES OF PERSONAL DATA PROTECTION," *The European Journal of Applied Economics* 19, no. 1 (2022).

organizational measures to mitigate data security risks. As such, this research not only contributes to the scientific literature, but also has a direct impact in encouraging more secure and sustainable e-commerce practices, both in the pre- and post-storage processing of personal data. This is important to analyze, given the rise of personal data-related crimes in Indonesia, underscoring the importance of integrating robust data protection measures into the existing legal framework.[16] Based on the background as stated above, the research questions of this study are (1) How is the Risk of Personal Data Processing on E-Commerce Sites Before Personal Data Storage? and (2) How is the Risk of Personal Data Processing on E-Commerce Sites After Personal Data Storage?

Method

This research is limited to the stages of personal data processing as described in Law Number 27 Year 2022 on Personal Data Protection. This research aims to analyze the forms of risks that can occur at each stage of personal data processing in E-Commerce applications. Scientific research uses one of the grand method sections, namely Library Research which is based on literature. Based on the subject of study and the type of problem, of the 3 (three) types of grand methods mentioned above, this research will use the Library Research method. Regarding this kind of research, it is also commonly called "Legal Research".[17] This kind of legal research does not recognize field research (field research) because what is studied is legal material so that it can be said to be library based, focusing on reading and analysing of the primary and secondary materials.[18] Primary data used in

[16] 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 and Society* 3, no. 1 (2024): 85–118.
[17] Soerjono Soekanto and Sri Mamudji, *Penelitian Hukum Normatif Tinjauan Singkat* (Jakarta: Rajawali Press, 2006).
[18] Jhony Ibrahim, *Teori Dan Metodologi Penelitian Hukum Empiris* (Malang: Bayumedia Publishing, n.d.).

this research are current regulations and secondary data used are articles and journals.

Result and Discussions

Risks of Personal Data Processing on E-Commerce Websites Prior to Personal Data Storage

Acquisition and Collection Phase of Personal Data

The first risk in the personal data acquisition and collection phase is related to the transparency of data collection by the personal data controller. As stipulated in the provisions of Law Number 27 Year 2022 on Personal Data Protection (PDP Law), the matter that must be followed by the Organizer in the acquisition and collection of personal data is the transparency of data collection.[19] This transparency can be in the form of clear information to the Data Subject about the purposes, benefits, and risks of the processing of personal data to be carried out by the Organizer.

To provide protection for personal data, the PDP Law regulates every thing that must be done and fulfilled by the controller of personal data in the course of processing personal data. Preventive efforts focus on the obligation of the personal data controller and/or processor to do and/or not do something related to the personal data it processes. Acquisition and collection and at this other stage can be both specific personal data and general personal data. 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, personal financial data, and/or other data in accordance with applicable laws. Whereas general personal data includes full name, gender, nationality, religion, marital

[19] Gita Theresa, "Perlindungan Hukum Terkait Data Pribadi Dalam Penyelenggaraan Fintech P2P Lending Di Indonesia," *Jurnal Darma Agung* 32, no. 3 (2024): 353–65.

status and/or personal data combined to identify a person.[20] Meanwhile, in terms of personal data collection on e-commerce websites, personal data that is generally collected according to the type of personal data according to Law Number 27 of 2022 is biometric data, personal financial data, full name, gender, nationality, and personal data combined to identify a person.

Other risks that can occur at the stage of obtaining and collecting personal data are related to data collection that is not specific, unlimited, and illegal. Data collection must be specific and any subsequent use of the data must be limited to the specific purpose. This has the adverse impact of misuse of data for unapproved purposes and excessive processing that overloads the system. In addition, the collection of personal data should also be limited. The restriction of data collection in this case means that the data should not be made publicly available or used for purposes beyond the specific purpose except with the consent of the data owner or the approval of the legal authority.[21]

Data collection that does not have a clear or specific purpose can lead to serious problems, such as the use of data for unintended or even illegal purposes. Excessive data collection increases the complexity of management and storage, and increases the chance of data falling into inappropriate hands such as cyberattacks or internal negligence. So in this case it is necessary to pay special attention that data collection must be specific, limited, and legal.[22] In this phase, it is also important to pay attention to the privacy policy that has been created. Privacy Policy/Privacy Statement/Privacy Notice is an agreement between digital platform providers and users. Digital platform users are considered to have bound

[20] Putra and Fibrianti, "Threats and Legal Protection of Personal Data Combined in E-Commerce Transactions Based on Personal Data Protection Law in Indonesia."
[21] Gilbert Kosegeran, "Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin," *Lex Privatum* 9, no. 12 (2021).
[22] Theresa, "Perlindungan Hukum Terkait Data Pribadi Dalam Penyelenggaraan Fintech P2P Lending Di Indonesia."

themselves to the provisions in the privacy policy.[23] Even though digital platform users only visit the website, they have bound themselves through the privacy policy.[24]

Processing and Analyzing Personal Data Phase

In terms of processing, there is potential for crime in the development of technology and information as well as in the data and information management sector, especially in the management of personal data that requires data protection. The advancement of information and communication technology has made the boundaries of privacy thinner, this is further magnified by the management of personal data which is basically carried out dynamically. Various personal data are increasingly easy to spread.[25] This can have an impact on the open access of personal data belonging to the subject of personal data in the public space.

Another risk that can occur at the processing and analyzing stage is the occurrence of damage to the database and hardware components causing the data to be inaccessible. This can have an impact on the obstruction of personal data processing.[26]

Risks of Personal Data Processing on E-Commerce Websites After The Storage of Personal Data

Personal Data Retention Phase

Another principle is that the processing of personal data must be carried out by ensuring the security of personal data from unauthorized

[23] Edmon Makarim, *Pengantar Hukum Telematika: Suatu Kompilasi Kajian* (Depok: PT Raja Grafindo Persada, 2005).
[24] Rama Dhianty, "Kebijakan Privasi (Privacy Policy) Dan Peraturan Perundang-Undangan Sektoral Platform Digital Vis a Vis Kebocoran Data Pribadi," *Scripta: Jurnal Kebijakan Publik Dan Hukum* 2, no. 1 (2022): 186–99.
[25] Aswandi, Muchin, and Sultan, "Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS)."
[26] Iqbal Santosa and Raras Yusvinindya, "Risk Analysis and Control of Personal Data Protection in the Population Administration Information System," *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)* 3, no. 3 (2019): 496–504.

access, disclosure in an unauthorized manner, unauthorized modification, misuse, destruction, and deletion of personal data as a form of personal data storage risk.[27] The data recorded in storage is not only about personal data, but also includes image data, sound, and even electronic data such as conversation history.[28] So that attacks can also occur on this data in addition to personal data. In general, the leakage of data can occur through intrusion of access from outside which access to the system.[29]

In addition, there are risks of logical attacks, virus attacks and Denial of Service (DoS) attacks at the storage stage of personal data processing that cause data loss/exposure.[30] Logical attacks are attempts to hack the system by looking for weaknesses in computer applications or programs, such as trying to guess passwords or exploiting security holes in the software. Meanwhile, a virus attack is a form of spreading a malicious program that can duplicate itself and spread to other computers, which can damage or steal data on the infected system. Meanwhile, a DoS attack is an attempt to flood the system with so many access requests that the server is unable to serve legitimate users and eventually the system becomes dysfunctional. Many sources are used in the data analysis process in collecting the data, so it is necessary to maintain privacy.[31] Misuse of data by unauthorized parties can have a negative impact on consumers.[32]

Personal Data Repair and Update Phase

[27] Theresa, "Perlindungan Hukum Terkait Data Pribadi Dalam Penyelenggaraan Fintech P2P Lending Di Indonesia."
[28] Sandryones Palinggi and Erich C Limbongan, "Pengaruh Internet Terhadap Industri Ecommerce Dan Regulasi Perlindungan Data Pribadi Pelanggan Di Indonesia," in *Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi)*, vol. 4, 2020.
[29] Achmad Rafli Hidayah, "SANKSI TERHADAP PENYELENGGARA E-COMMERCE APABILA GAGAL DALAM MELINDUNGI DATA PRIBADI PENGGUNA," *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, no. 2 (2022): 397–410.
[30] Iqbal, Loc.Cit.
[31] Iqbal, Loc.Cit.
[32] M Sahlan and Muhammad Irwan Padli Nasution, "Hubungan Antara Kesadaran Privasi Data Pribadi Dan Penggunaan Layanan PayLater Di Kalangan Pengguna E-Commerce Di Indonesia," *JOURNAL SAINS STUDENT RESEARCH* 2, no. 4 (2024): 271–78.

In the case of repairing and updating personal data, there is a risk of data input errors and lack of validation and verification. The systems used and the controllers of personal data have a big role to play in addressing these issues. Systems and controllers should enable accurate rectification and updating of personal data.[33] Rectification and updating of personal data is important to provide validity to rules according to the substance of national law. The substance of national law can have a pluralistic nature, but this plurality still has the same source of validity, namely the 1945 Constitution. Humans have a big role to play in efforts to improve and update personal data. In this case, the Ponemo Institute states that most personal data breaches occur due to human error.[34] This can have an impact on data inconsistency on an ongoing basis so that data improvement and updating becomes important to do to handle personal data risks.

Appearance, Announcement, Transfer, Dissemination or Disclosure Phase of Personal Data

There are several personal data processing risks in the display, announcement, transfer, dissemination, or disclosure of personal data. In terms of the display of personal data, there is a risk of personal data being displayed by a party that should not be in the internal control of personal data. In this case, an example is unauthorized staff trying to enter the system.[35] In addition, there is also the risk of announcement, transfer, dissemination, and disclosure of personal data as a form of personal data processing. The risk of announcement in this case is when a personal data controller announces in a one-way manner more data belonging to a personal data subject than should be announced. Meanwhile, transfer is

[33] Duarte Gonçalves-Ferreira et al., "OpenEHR and General Data Protection Regulation: Evaluation of Principles and Requirements," *JMIR Medical Informatics* 7, no. 1 (2019): e9845.
[34] Pratiwi Agustini, "34 Persen Pelanggaran Data Pribadi Akibat Human Error," aptika.kominfo.go.id, 2020, https://aptika.kominfo.go.id/2020/08/34-persen-pelanggaran-data-pribadi-akibat-human-error/.
[35] Iqbal, Loc.Cit.

intended as a form of moving personal data from one system/location/organization to another system/location/organization. Transfers can occur between departments, between companies, or even between countries. Distribute personal data to various parties or make the data available for wider access. Unlike transfer which is more specific in its purpose and recipients, dissemination usually covers a wider public. In this case, human error is a direct and/or indirect cause of the incident, including both intentional and unintentional error.[36] It can also be caused by software malfunction.[37] Such software malfunctions may result in the incorrect display, announcement, transfer, dissemination, or disclosure of personal data. Until the final impact on personal data that cannot be accessed.[38]

Phase of deletion or destruction of personal data

Personal data that is revealed due to the inefficient retention/archiving/disposal of information.[39] The deletion and destruction of personal data is closely related to delisting from search engines. This is related to the request to remove data (right to delisting) from search engines such as Google as stipulated in Article 17 of Government Regulation Number 71 of 2019.[40] This has the risk of revealing personal data belonging to the personal data subject in the public space through search engines and the data that should be deleted can be accessed again by the system belonging to the personal data controller. Furthermore, based on the provisions of Article 42, the Personal Data Controller shall terminate the processing of personal data in the event that it has reached the retention period, has

[36] Khando Khando et al., "Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review," *Computers & Security* 106 (2021): 102267.
[37] Santosa and Yusvinindya, "Risk Analysis and Control of Personal Data Protection in the Population Administration Information System."
[38] Iqbal, Loc.Cit.
[39] Iqbal, Loc.Cit.
[40] Muhammad Taufik Ajiputera and Heru Susetyo, "Implementasi Pengaturan Hak Untuk Dilupakan Melalui Sistem Penghapusan Data Pribadi Dan / Atau Dokumen Elektronik Menurut Perspektif Hukum Positif Di Indonesia" 6, no. 3 (2024): hlm 8063-8065.

achieved the purpose of processing personal data, or there is a request from the personal data subject. Personal data under Article 43 shall be erased by the personal data controller in the case of (a) The Personal Data is no longer necessary for the achievement of the purposes of the Personal Data processing; (b) The Personal Data Subject has withdrawn consent to the processing of Personal Data; and (c) there is a request from the Personal Data Subject; or the Personal Data is obtained and/or processed unlawfully.

In addition, personal data under Article 44 shall be destroyed by the personal data controller in the case of (a) has expired its retention period 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 is obtained and/or processed by unlawful means.

In terms of deletion and destruction of personal data, there is also a problem that there is no special institution that handles the system for deleting personal data that has been spread on the internet and there are no definite rules for application providers in Indonesia to be responsible for deleting data at the request of data subjects.[41] This creates a risk that personal data that should no longer be used can still be accessed and misused. By bringing experts from different areas, companies can ensure a comprehensive approach to compliance that takes into account legal requirements, technical capabilities, and organizational policies.[42] The ideal regulatory design can prevent data breaches.[43] Proper security measures can help protect users' personal data from being compromised. Either by strengthening the system, updating the system regularly, or increasing the capacity of human resources who process personal data. E-Commerce that

[41] Ibid.
[42] E G Chukwurah and S Aderemi, "Harmonizing Teams and Regulations: Strategies for Data Protection Compliance in US Technology Companies," *Computer Science & IT Research Journal* 5, no. 4 (2024): 824–38.
[43] Dona Budi Kharisma and Alvalerie Diakanza, "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union," *International Journal of Human Rights in Healthcare* 17, no. 2 (2024): 157–69.

has a good reputation in the market, with a positive image that adds confidence to the security and integrity of the platform. Maintaining the security of customer data during online transactions is very important to maintain integrity and trust in the e-commerce ecosystem.[44]

Conclusion

In E-Commerce applications, there are different risks at each stage of processing personal data interpreted based on Law No. 27 of 2022, both at the stage of processing personal data before storage and after storage up to the stage of deletion and destruction of personal data itself. Prior to the storage of personal data, three risks that can occur include data collection that is not in accordance with applicable regulations, the absence of transparency of data collection, and data collection that is not specific, unlimited, and illegal. As for the risk of processing personal data, the three risks that can occur are unauthorized access, disclosure in an unauthorized manner, unauthorized modification, misuse, destruction, and loss of personal data on the system. Appropriate security measures can help protect users' personal data from being compromised. Either by strengthening the system, updating the system regularly, or increasing the capacity of human resources who process personal data.

References

Agustini, Pratiwi. "34 Persen Pelanggaran Data Pribadi Akibat Human Error." aptika.kominfo.go.id, 2020. https://aptika.kominfo.go.id/2020/08/34-persen-pelanggaran-data-pribadi-akibat-human-error/.

[44] Nasywa Chintami Rahmadani Putri et al., "Strategi Peningkatan Keamanan Data Pelanggan Dalam Penjualan Online Di Tokopedia," *Jurnal Siber Multi Disiplin* 2, no. 1 (2024): 54–67.

Ajiputera, Muhammad Taufik, and Heru Susetyo. “Implementasi Pengaturan Hak Untuk Dilupakan Melalui Sistem Penghapusan Data Pribadi Dan / Atau Dokumen Elektronik Menurut Perspektif Hukum Positif Di Indonesia” 6, no. 3 (2024): hlm 8063-8065.

Aswandi, Ririn, Purti Rofifah Nabilah Muchin, and Muhammad Sultan. “Perlindungan Data Dan Informasi Pribadi Melalui Indonesian Data Protection System (IDPS).” *Jurnal Legislatif*, 2020, 167–90.

Chukwurah, E G, and S Aderemi. “Harmonizing Teams and Regulations: Strategies for Data Protection Compliance in US Technology Companies.” *Computer Science & IT Research Journal* 5, no. 4 (2024): 824–38.

Dana, Haris Satrio, Baginda Akbar Edison, Halim Darajat, and Helfira Citra. “Perlindungan Konsumen Dalam Perdagangan Elektronik (e-Commerce).” *Jurnal Kajian Hukum Dan Pendidikan Kewarganegaraan| E-ISSN: XXXX-XXX* 1, no. 1 (2024): 82–86.

Dhianty, Rama. “Kebijakan Privasi (Privacy Policy) Dan Peraturan Perundang-Undangan Sektoral Platform Digital Vis a Vis Kebocoran Data Pribadi.” *Scripta: Jurnal Kebijakan Publik Dan Hukum* 2, no. 1 (2022): 186–99.

Dokuchaev, Vladimir A, Victoria V Maklachkova, and V Yu Statev. “Classification of Personal Data Security Threats in Information Systems.” *T-Comm-Телекоммуникации и Транспорт* 14, no. 1 (2020): 56–60.

Gonçalves-Ferreira, Duarte, Mariana Sousa, Gustavo M Bacelar-Silva, Samuel Frade, Luís Filipe Antunes, Thomas Beale, and Ricardo Cruz-Correia. “OpenEHR and General Data Protection Regulation: Evaluation of Principles and Requirements.” *JMIR Medical Informatics* 7, no. 1 (2019): e9845.

Hidayah, Achmad Rafli. “SANKSI TERHADAP PENYELENGGARA E-COMMERCE APABILA GAGAL DALAM MELINDUNGI DATA

PRIBADI PENGGUNA." *Bureaucracy Journal: Indonesia Journal of Law and Social-Political Governance* 2, no. 2 (2022): 397–410.

Hidayat, Topik, Jeffry A Ch Likadja, and Petrus E Derozari. "PERLINDUNGAN HUKUM DATA PRIBADI KONSUMEN DALAM PERDAGANGAN ELEKTRONIK." *Journal of Comprehensive Science (JCS)* 2, no. 5 (2023).

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

Khando, Khando, Shang Gao, Sirajul M Islam, and Ali Salman. "Enhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review." *Computers & Security* 106 (2021): 102267.

Kharisma, Dona Budi, and Alvalerie Diakanza. "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union." *International Journal of Human Rights in Healthcare* 17, no. 2 (2024): 157–69.

Kosegeran, Gilbert. "Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin." *Lex Privatum* 9, no. 12 (2021).

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.

Makarim, Edmon. *Pengantar Hukum Telematika: Suatu Kompilasi Kajian*. Depok: PT Raja Grafindo Persada, 2005.

Pahlevi, Reza. "Nilai Transaksi E-Commerce Indonesia Diperkirakan Capai US $137, 5 Miliar Pada 2025." *Databoks. Katadata. Co. Id*, 2022.

Palinggi, Sandryones, and Erich C Limbongan. "Pengaruh Internet Terhadap Industri Ecommerce Dan Regulasi Perlindungan Data Pribadi Pelanggan Di Indonesia." In *Semnas Ristek (Seminar Nasional Riset Dan Inovasi Teknologi)*, Vol. 4, 2020.

Priliasari, Erna. “Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce.” *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional* 12, no. 2 (2023).

Priscyllia, Fanny. “Perlindungan Privasi Data Pribadi Perspektif Perbandingan Hukum.” *Jatiswara* 34, no. 3 (2019): 239–49.

Puspita, Khafidah. “Perlindungan Hukum Data Pribadi Konsumen Dalam Perjanjian Pinjaman Online Di Indonesia.” *Jurisprudensi: Jurnal Ilmu Syariah, Perundang-Undangan Dan Ekonomi Islam* 15, no. 2 (2023): 67–83.

Putra, Tegar Islami, and Nurul Fibrianti. “Criminalization of Consumers for Criticism Given to Companies Through Cyberspace in Theoretical Studies: Kriminalisasi Konsumen Atas Kritik Yang Diberikan Kepada Perusahaan Melalui Dunia Maya Dalam Kajian Teoritis.” *Annual Review of Legal Studies* 1, no. 2 (2024): 179–204.

———. “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.

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 and Society* 3, no. 1 (2024): 85–118.

Putri, Nasywa Chintami Rahmadani, Achmad Fauzi, Muhammad Khadir Ali, Nazwa Aulia Ramadhan, Putri Jasmine Salsabilla, Latifah Julia Cahya, and Farah Aulia Ernawati. “Strategi Peningkatan Keamanan Data Pelanggan Dalam Penjualan Online Di Tokopedia.” *Jurnal Siber Multi Disiplin* 2, no. 1 (2024): 54–67.

Sahlan, M, and Muhammad Irwan Padli Nasution. “Hubungan Antara Kesadaran Privasi Data Pribadi Dan Penggunaan Layanan PayLater Di Kalangan Pengguna E-Commerce Di Indonesia.” *JOURNAL SAINS STUDENT RESEARCH* 2, no. 4 (2024): 271–78.

Santosa, Iqbal, and Raras Yusvinindya. "Risk Analysis and Control of Personal Data Protection in the Population Administration Information System." *Jurnal RESTI (Rekayasa Sistem Dan Teknologi Informasi)* 3, no. 3 (2019): 496–504.

Setiawan, Herdi, Mohammad Ghufron, and Dewi Astutty Mochtar. "Perlindungan Hukum Terhadap Data Pribadi Konsumen Dalam Transaksi E-Commerce." *MLJ Merdeka Law Journal* 1, no. 2 (2020): 102–11.

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

Theresa, Gita. "Perlindungan Hukum Terkait Data Pribadi Dalam Penyelenggaraan Fintech P2P Lending Di Indonesia." *Jurnal Darma Agung* 32, no. 3 (2024): 353–65.

Vicentijevic, Kosana. "GDPR AND CHALLENGES OF PERSONAL DATA PROTECTION." *The European Journal of Applied Economics* 19, no. 1 (2022).

***

DECLARATION OF CONFLICTING INTERESTS

None

FUNDING INFORMATION

None

ACKNOWLEDGMENT

None

HISTORY OF ARTICLE

Submitted : January 20, 2025

Revised : March 2, 2025

Accepted : April 19, 2025

Published : May 1, 2025