IJLR: International Journal of Law Reconstruction
Volume 8, Number 2, September 2024
DOI: http://dx.doi.org/10.26532/ijlr.v8i2.32711

CONSENT OF E-WALLET PERSONAL DATA SUBJECTS ON CROSS-BORDER DATA TRANSFER

Kadek Ary Purnama Dewi
Universitas Udayana, Denpasar, Indonesia
aryartana2213@gmail.com

Ni Ketut Supasti Dharmawan
Universitas Udayana, Denpasar, Indonesia
supasti_dharmawan@unud.ac.id

Abstract

Indonesia has the highest usage of electronic wallets (e-wallets) in Southeast Asia. However, e-wallets, as mobile payment services, pose risks and challenges for users. The submission of personal data by users and the acceptance of this data by e-wallet providers are legally enforceable expressions of intent. Protecting personal data on e-wallets is essential to safeguard human rights and ensure justice for consumer justice. This study employs normative juridical research methods, including analytical and conceptual approaches, the statute approach, and comparative analysis. A literature review was conducted, gathering primary and secondary legal materials, which were then analyzed qualitatively. The legal source that is the focus of this research is Law Number 27 of 2022 concerning Personal Data Protection. The findings indicate that the future regulatory model for personal data protection on e-wallets should include requirements for user consent in data transfer activities, both domestically and internationally. Technical guidelines for personal data protection in e-wallets should be formalized within Bank Indonesia Regulations and Financial Services Authority Regulations.

Keywords: E-Wallet; Mobile Payment; Personal Data; Protection

A. INTRODUCTION

Indonesia has the highest number of e-wallet users in Southeast Asia. However, as Claudel Mombeuil[1] states, growing concerns over the collecting and sharing of users' personal information have accompanied the rapid expansion of mobile payments.[2] These growing concerns typically on the security and privacy of users' personal information, often collected by businesses whose models and revenue streams depend heavily, if not entirely, on trading users' personal information (such as data mining companies and

[1] Claudel Mombeuil., An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets, *Journal of Retailing and Consumer Services*, Vol.55, no.3, 2020, page. 102127

[2] Augi Ciptarianto and Yudo Anggoro., E-Wallet application penetration for financial inclusion in Indonesia, *International Journal of Current Science Research and Review*, Vol.5, no. 2, 2022, page. 319-332.

suppliers).

E-wallets operate through an internet-connected system, making them very convenient for consumers to use. They function much like physical wallets, serving as a place to store various types of information, such as account numbers, e-money cards, personal identities, contact details, transaction history, billing information, customer accounts, and other data needed for e-commerce transactions. To use an e-wallet, users simply enter their data during the initial registration and can then connect to any site for transactions. E-wallets enhance in-store efficiency with the convenience they offer.[3] According to Teng and Khong[4], successful e-wallet business model measures include a user-friendly interface, promotional campaigns and customer service. In addition to the obvious convenience for both consumers and companies, e-wallets as mobile payment services present certain risks and challenges for their users. Financial technology companies providing these services have direct access to transaction data from millions of consumers. For example, when shopping online, users of financial technology services are often required to provide their full name, shipping address, payment method, and payment information.[5]

The act of sending personal data by the user and receiving it by the e-wallet application provider is regarded as a legally enforceable statement of intent. Article 12, paragraph (1) of the UNCITRAL Model Law on Electronic Commerce, 1996, regulates parties' recognition of data messages.[6] The protection of personal data is a form of consumer protection. Consumer protection refers to the legal safeguarding of consumer rights. Protecting consumer rights is an effort to provide access to justice for consumers, who often find themselves in an inferior position. While information technology offers significant benefits, it also leads to various legal challenges.[7] Violation of personal data is a violation of one's privacy. This causes harm to consumers. Akanfe, Valecha, and Rao[8] said that in this digital world, data privacy is mostly applicable to critical personal information, which may include personal identification numbers, social security numbers, financial records, credit cards, etc. However, the privacy rights of citizens vary from one country to the next. Protecting personal data in e-wallets is essential to ensure legal certainty, especially as human activities shift from conventional to digital in the era of Industrial Revolution 5.0. The government's non-cash

[3] Rohmatun Ni'mah and Indah Yuliana., E-Wallet: Sistem Pembayaran Dengan Prinsip Hifzul Maal, *Jurnal Ekonomi Syariah*, Vol.5, no. 2, 2020, page. 52-66.

[4] Teng, Shasha, and Kok Wei Khong., Examining actual consumer usage of E-wallet: A case study of big data analytics, *Computers in Human Behavior*, Vol.121, no.4, 2021, page. 106778.

[5] Fidhayanti, Dwi., Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data/Informasi Konsumen Financial Technology Pada Sektor Mobile Payment, *Jurisdictie*, Vol.11, no. 1, 2020, page. 16-47

[6] Wijayanti, Fika Arum, and Budi Santoso., The Analysis Of The Notary's Responsibilities For The Storage Of Electronic Deed Minuta, *Jurnal Hukum Volkgeist*, Vol.8, no. 1, 2023, page. 85-91.

[7] Theixar, Regina Natalie, and Ni Ketut Supasti Dharmawan., Tanggung Jawab Notaris Dalam Menjaga Keamanan Digitalisasi Akta, *Acta Comitas: Jurnal Hukum Kenotariatan*, Vol.6, no. 01, 2021, page. 1-15.

[8] Oluwafemi Akanfe, Rohit Valecha, and H. Raghav Rao., Design of a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services, *IEEE Transactions on Engineering Management*, Vol.70, No. 3, 2020, page. 864-876.

policy must be balanced with consumer protection policies regarding personal data in e-wallet usage. The absence of comprehensive personal data laws enables business actors to request irrelevant personal information, which is then often freely traded, ultimately harming consumers. Personal data protection is a matter of human rights and upholds the values of justice for consumers.[9] In protecting personal data, of course, personal data consent is needed in data transfer activities. A personal data subject is an individual to whom personal data is attached.

Law No. 27 of 2022 on Personal Data Protection does not fully require the consent of personal data subjects for data transfer activities. Article 56 of this law stipulates that in transferring personal data, the Personal Data Controller must ensure that the country of domicile of the receiving Personal Data Controller and/or Processor has a level of personal data protection equal to or higher than that provided in this law. The Personal Data Controller must ensure adequate and binding personal data protection if these conditions are not met. Consent from the personal data subject is required only if both of these conditions are not satisfied. This provision could permit cross-border personal data breaches.

B. RESEARCH METHODS

This study is a normative juridical research that examines issues related to legal subjects' consent in transferring personal data on e-wallets. The primary legal source for this research is Law Number 27 of 2022 concerning Personal Data Protection. This research employs analytical and conceptual approaches, as well as the statute and comparative approaches, analyzing the issue by comparing provisions with other WTO member countries with personal data protection laws, namely the United States, the United Kingdom, and Malaysia. Primary legal materials include legislation and official records or minutes from the legislative process, while secondary materials consist of scientific journals and legal literature relevant to this discussion. A literature review was conducted on both primary and secondary legal materials. After collecting all legal materials, they were analyzed qualitatively.

C. RESULTS AND DISCUSSION

1. The Arrangement of Personal Data Protection in International Legal Instruments

The law of personal data protection develops in parallel with the development of technology itself, especially information and communication technology.[10] The right to data protection aims to safeguard individuals in the era of the information society. Germany was the first country to pass a Data Protection Law in 1970, followed by the UK in the same year, and then several other European countries, including Sweden, France, Switzerland, and Austria. Similar developments occurred in the United States with the

[9] Michael Veale, Reuben Binns, and Jef Ausloos., When data protection by design and data subject rights clash, *International Data Privacy Law*, Vol.8, no. 2, 2018, page. 105-123.

[10] Diana Setiawati, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga., Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore, *Indonesian Comparative Law Review*, Vol.2, no. 2, 2020, page. 95-109.

Fair Credit Reporting Act in 1970, which also included data protection elements. In the following decade, various regional organizations began to address the issue of personal data protection, including the establishment of The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108) in 1981 (amended in 2018), the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data in 1980 (amended in 2013), and the Guidelines for the Regulation of Computerized Personal Data Files (General Assembly resolution 45/95 and E/CN.4/1990/72). APEC (Asia-Pacific Economic Cooperation) issued the APEC Privacy Framework in 2004, later amended in 2015.[11]

Discussions on personal data protection continue to increase at international, regional, and national levels. International and regional organizations publish recommendations that serve as guidelines for member countries. These recommendations have also influenced the establishment of personal data protection regulations in various countries, such as the OECD Privacy Framework published by the Organization for Economic Co-Operation and Development (OECD) in 1980 and revised in 2013. The Framework on Personal Data Protection was agreed upon at the regional level during the ASEAN Telecommunications and Information Technology Ministers Meeting (Telmin).[12] Several multilateral legal instruments governing internationally recognized data privacy principles have laid the foundation for modern national data protection laws. Some of these instruments have evolved to include specific data privacy provisions, while others provide general rules covering a range of issues related to privacy. International treaties protecting privacy include the Organization for Economic Co-operation and Development (OECD) Privacy Guidelines and the European Convention for the Protection of Human Rights of 1950.[13]

The OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data is the first statement on data protection, outlining principles and minimum standards for member countries. However, this instrument is not a hard law and does not have legally binding force; it serves only as a set of recommendations or guidelines for OECD member countries.[14] The Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013) emphasizes that the principles outlined in these Guidelines are

[11] Wahyudi Djafar, Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan, in Public Lecture on "Tantangan Hukum dalam Era Analisis Big Data," Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada, 2019, http://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf

[12] Siti Yuniarti., Perlindungan hukum data pribadi di Indonesia, *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, Vol.1, no. 1, 2019, page. 147-154.

[13] Dijan Widijowati and Sergiy Denysenko., Securing Consumer Rights: Ethical and Legal Measures against Advertisements that Violate Advertising Procedures, *Lex Publica*, Vol.10, no. 1, 2023, page. 28-42.

[14] Eliezher Nathaniel and I. Gede Putra Ariana., Aspek Perlindungan Hukum Internasional Data Pribadi Pengguna Layanan Jejaring Sosial dan Kewajiban Korporasi Penyedia Layanan, *Jurnal Kertha Desa*, Vol.9, no.7, 2023, page. 88-103.

complementary and should be considered collectively. The interpretation of these principles should not limit the application of various protective measures to specific categories of personal data based on their nature or the context in which they are gathered, stored, processed, or distributed. Additionally, the principles should not be construed in a manner that unreasonably restricts the freedom of expression.

The Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013) [C (80)58/FINAL, as amended on July 11, 2013, by C (2013) 79] places obligations on member states as set out in Article 19. In implementing these Guidelines, Member countries should:

a) develop national privacy strategies that reflect a coordinated approach across governmental bodies;
b) adopt laws protecting privacy;
c) establish and maintain privacy enforcement authorities with the governance, resources and technical expertise necessary to exercise their powers effectively and to make decisions on an objective, impartial and consistent basis;
d) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
e) provide for reasonable means for individuals to exercise their rights;
f) provide for adequate sanctions and remedies in case of failures to comply with laws protecting privacy;
g) consider the adoption of complementary measures, including education and awareness raising, skills development, and the promotion of technical measures that help to protect privacy;
h) consider the role of actors other than data controllers in a manner appropriate to their individual role; and
i) ensure that there is no unfair discrimination against data subjects.

Asean Telecommunications and Information Technology Ministers Meeting (Telmin) Framework on Personal Data Protection is an international agreement among Southeast Asian countries. The Participants will endeavour to cooperate, promote and implement in their domestic laws and regulations the Principles of Personal Data Protection as set out in Paragraph 6 of this Framework (herein referred to as principles) while continuing to ensure and facilitate the free flow of information among the ASEAN Member States. This Framework will not apply to:

(a) Measures adopted by a Participant to exempt any areas, persons or sectors from the application of the Principles; and
(b) Matters relating to national sovereignty, national security, public safety, public policy, and all government activities deemed suitable by a Participant are to be exempted.

States in the United States have provisions for personal data protection. Jie Huang, in his research, states that GDPR-style uniform data protection laws do not exist in the USA. Instead, the applicable state-based

legislation in the state where the data subject resides may also apply to a foreign company that obtains, maintains, transmits, processes, or shares a U.S. resident's personal information. Therefore, it is necessary to evaluate each U.S. data protection law separately to determine whether it aligns with public policy.[15]

The United States has not fully embraced EU data protection efforts. The EU's omnibus approach to data protection is based on individual rights to data, detailed rules, default bans on data processing, and strong adherence to fair information practices. In contrast, the patchwork approach in the United States is more permissive, uncertain, and centered on the vulnerabilities of individuals in their commercial relationships with companies. William McGeveran uses this distinction to differentiate between European "data protection" and American "data protection." American and European regulators have long tried to navigate this distinction to the best of their abilities.[16] Data privacy protection is also applicable to the use of e-wallets in the United States. Some of the dominant e-wallets in the country include American Express, PayPal, and eBay. In 2022, the United States Senate introduced a bill on e-wallets called the "Banking For All Act." This bill offers definitions for digital dollars and digital dollar wallets, and it includes provisions requiring all member banks to open and maintain digital dollar wallets for everyone.[17]

The "Banking For All Act" defines a "digital dollar wallet" as a digital wallet or account maintained by a Federal Reserve bank on behalf of any individual for the purpose of holding digital dollar balances. The bill also references the privacy provisions of the Privacy Act of 1974, stating that Section 552a of Title 5 of the United States Code will apply to digital dollar wallets. This means that the privacy obligations for each Federal Reserve bank and its employees will align with those concerning federal tax returns, as specified in sections 6103, 7213(a)(1), 7213A, and 7431 of the Internal Revenue Code of 1986, ensuring that strict privacy protections and potential penalties are in place for the handling of personal data.

The UK regulates personal data protection through the Data Protection Act 1998, which came into force in 2000. This provision replaced the previous regulation, the Data Protection Act 1984. In the UK, there is an implementing body known as the Data Protection Commissioner, which is responsible for overseeing all data users who control personal data. As part of the European Union, the UK previously adhered to a compilation of EU regulations. The EU digital wallet app is designed to store payment-related data and users' passwords securely. Every citizen in the 27 EU member states will have a single online identity to use the app and log in to government websites. Citizens of EU member states can also use

[15] Jie Huang., Conflicts and tentative solutions to protecting personal data in investment arbitration, *European Journal of International Law*, Vol.32, no. 4, 2021, page. 1191-1220.

[16] Woodrow Hartzog and Neil Richards, Privacy's Constitutional Moment and The Limits of Data Protection, *Boston College Law Review*, Vol.61, No. 5, 2020, page. 1688-1761.

[17] Jason Brett, Digital Dollar and Digital Wallet Bill Surfaces in The U.S. Senate, 2020, https://www.forbes.com/sites/jasonbrett/2020/03/24/digital-dollar-and-digital-wallet-legislation-surfaces-in-the-us-senate/?sh=51220ca3866a

fingerprint and retina scanners to access the EU digital wallet.[18]

The UK, as part of the European Union, adopted the General Data Protection Regulation (GDPR), which implemented personal data protection rules in May 2018. The principles outlined in the EU GDPR were also discussed by technology and personal data protection law expert Berend van der Eijk, who emphasized the principle of transparency: citizens have the right to access, amend, and delete their personal data at any given time from a company's customer database. Additionally, companies are required to be transparent about why they collect data and how they will use it. The GDPR provides personal data protection in relation to sensitive categories such as race, ethnicity, political opinions, health, gender, and sexuality.[19] The EU General Data Protection Regulation (EU GDPR) encompasses several key components that govern personal data protection. It outlines essential principles for data management and establishes a classification system for general and specific types of personal data. The regulation defines the rights of personal data owners, ensuring they have control over their information. It also specifies the responsibilities of data controllers and processors in handling personal data and introduces guidelines for codes of conduct and certification processes. Furthermore, the GDPR addresses the transfer of personal data to other countries or international organizations, ensuring that adequate protections are in place. An independent supervisory authority is established to oversee compliance, and the regulation includes provisions for compensation, liability, and sanctions in cases of violations.

The GDPR specifies the scope of personal data, which includes name, identity number, location data, online identifier, or one or more specific physical components, physiological, genetic, mental, economic, cultural or social characteristics of an individual.[20] Furthermore, the scope of personally identifiable data in the GDPR includes data that is not directly identifiable but can be linked to an individual through the use of additional information, a process known as pseudonymization. The Information Commissioner's Office in the United Kingdom does not enforce an absolute right to delete electronic data and/or information about a person. As a result, the deletion of such data is not carried out by the electronic system provider, but rather by the search engine. The right to erasure does not confer an absolute right to be forgotten. Individuals have the right to retain personal data and prevent processing in certain circumstances, which, according to the Information Commissioner Office are as follows:

a. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
b. When the individual withdraws consent.

[18] Demis Rizky Gosta., Dompet Digital Uni Eropa, Aplikasi Milik Driver di New York, dan Lainnya, 2021, https://id.techinasia.com/dompet-digital-uni-eropa-aplikasi-milik-driver-di-new-york-dan-lainnya

[19] Hanifan Niffari., Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain), *Jurnal Yuridis*, Vol.7, No. 1, 2020, page. 105-119.

[20] H. Hasan and C. Mustafa., The Politics of Law of Sharia Economics in Indonesia, *Lex Publica,* Vol.9, no. 1, 2022, page. 30-57.

c. When the individual objects to the processing and there is no overriding legitimate interest in continuing the processing,
d. The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
e. The personal data has to be erased in order to comply with a legal obligation.
f. The personal data is processed in relation to the offer of information society services to a child.[21]

The Data Protection Act 1998, which replaced the Data Protection Act 1984, became effective on March 1, 2000. The Act was established in response to the rapid growth of computer use, which raised concerns about the processing of individuals' information without their knowledge and the lack of ability to access or correct that information if it was incorrect.[22] The Act sought to maintain a balance between the rights of individuals and the ability of others to process data about them. Changes from the previous law include the new law's applicability to manually processed data, not just data processed by computers. It also introduced the categorization of sensitive data and prohibited the transfer of data to countries that do not have sufficient data protection.[23]

The Data Protection Act 1998 also provides rights for data subjects, stating that any individual whose personal data is held by another person or party has the right to access that information, prevent the processing of their data, and seek compensation for any damage or harm caused by the data processing. Additionally, individuals have the right to restrict, prevent, delete, or destroy inaccurate data and can request the commissioner to mediate against violations of this Act. The Data Protection Act 1998 provisions also include exemptions related to national security, crime, taxation, health, education, and social work.

Malaysia already has a data protection law in place. Malaysia's first comprehensive personal data protection law, the Personal Data Protection Act 2010 (PDPA), was passed by the Malaysian Parliament on June 2, 2010, and came into force on November 15, 2013. The Personal Data Protection Act No. 709 of 2010 protects personal data in Malaysia. Sections 5 to 12 of the PDPA contain seven principles of personal data protection, namely: general principles of processing based on consent, notice and choice, disclosure, security, and data integrity (retention and access). These principles are more influenced by the EU Data Protection Directive than by the OECD Guidelines or APEC Framework.

The Personal Data Protection Act No. 709 of 2010 expressly protects the right to privacy of its citizens. General provisions are also set

[21] Information Commisioner Office, The Right to Erasure (The Right to be Forgotten), https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/

[22] Ninne Zahara Silviani, Rina Shahriyani Shahrullah, Vanessa Riarta Atmaja, and Park Ji Hyun., Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea, *Jurnal Hukum dan Peradilan*, Vol.12, no. 3, 2023, page. 517-546.

[23] Nadiah Tsamara., Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia dengan Beberapa Negara, *Jurnal Suara Hukum*, Vol. 3, No. 1, 2021, page. 53-84.

out in the Malaysian Penal Code, which prescribes fines or imprisonment of up to 5 years, or both, for individuals who interfere with the privacy of others. Malaysia's personal data law has been in effect since 2013, detailing the principles of personal data protection, the rights of data owners, the procedures for data transfer, and the obligations of parties that store data. It also regulates the complaint mechanism for individuals whose personal data has been unlawfully transferred.[24]

Malaysia established the Personal Data Protection Advisory Committee, as stipulated in the Data Protection Act 2010. This committee is responsible for receiving reports regarding the misuse and unlawful handling of personal data. Malaysia has also established a court of appeal for judicial resolution in this context. This law not only provides the right to protest but also imposes criminal penalties for anyone who violates the provisions designed to protect personal data owned by the public. One example of such sanctions is directed at those who unauthorizedly access or unlawfully collect personal data; offenders can face a maximum fine of five hundred thousand Malaysian ringgit and/or imprisonment for up to three years.[25]

In Malaysia's Personal Data Protection Act 2010, there is a rule requiring every individual or entity to apply for registration before managing consumers' personal data. Additionally, the Act contains provisions regulating cross-border transfers of personal data, stipulating that such transfers can only occur to countries that provide a high level of security or at least equivalent protection for personal data as that in Malaysia. Furthermore, the provisions regarding sanctions in the Personal Data Protection Act 2010 explicitly state that civil and criminal penalties apply to anyone who violates personal data protection.[26]

Personal data includes sensitive personal data and expressions of opinion about the data subject. However, it does not encompass any information processed for the purpose of credit reporting by credit reporting agencies under the Credit Reporting Agencies Act 2010. Local governments in Malaysia focus not only on the booming financial development in their regions but also on protecting consumer interests to ensure the healthy and transparent functioning of the financial industry. All e-wallet vendors must be licensed in accordance with the guidelines set forth by Bank Negara Malaysia and the Malaysian Securities Commission. Additionally, personal data protection in e-wallet regulations in Malaysia must include a password for access.[27]

[24] Muhammad Saiful Rizal., Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia, *Jurnal Cakrawala Hukum*, Vol.10, no. 2, 2019, page. 218-227.

[25] Y. Putra., Comparison of personal data protection laws using narrative policy framework between indonesia, malaysia, and Japan, *Negrei Academic Journal of Law and Governance*, Vol.2, no. 2, 2022, page. 99.

[26] Miftahul Jannah, F. Yudhi Priyo Amboro, and Rina Shahrullah., Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law, *Journal of Law and Policy Transformation*, Vol.8*,* no. 2, 2023, page. 89-97.

[27] Md. Mahmudul Alam, Ala Eldin Awawdeh, and Azim Izzuddin Bin Muhamad., Using e-wallet for business process development: challenges and prospects in Malaysia, *Business Process Management Journal*, Vol.27, no. 4, 2021, page. 1142-1162.

As national laws, as of January 2018, more than 100 countries have adopted data protection laws.[28] Data protection laws are generally structured around the scope and extent of data protection. This includes the scope of data controllers and processors, as well as territorial and jurisdictional reach; definitions and types of personal data; data protection principles, including the grounds for data processing; obligations of data controllers and processors; rights of data subjects; and supervision and enforcement, which is typically complemented by an independent supervisory authority (data protection authority).[29]

The provisions regarding personal data are regulated simply in Article 26 of Law No. 19 of 2016 on the Amendments to Law No. 11 of 2008 on Electronic Information and Transactions. This article states that, unless otherwise provided by laws and regulations, the use of any information through electronic media concerning a person's personal data must be done with the consent of the person concerned. The individual may file a lawsuit for losses incurred under this Law.

Anugerah and Indriani analyzed the potential risks to personal data. The risk regarding how data should be treated can be seen in the centralized authority, in this case, a fintech service provider, during several steps such as collecting, processing, and analyzing data. Even though the technology used in fintech, such as blockchain technology, can encrypt certain actions on the web, there are still potential threats in cyberspace. Cyber risk and cybersecurity are the main issues concerning consumer data protection; cyber-attacks can pose a threat to the system or data confidentiality, integrity, and availability. Moreover, these potential cyber-attacks are becoming more frequent and costly for society as a whole. The financial sector is one of the prime targets of cyber-attacks because it represents where the money is and symbolizes capitalism, which can lead to cyber-attacks that may have political motivations.[30]

Provisions regarding consumer protection in Indonesia are technically and juridically regulated by the Financial Services Authority Regulation Number: 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. Article 1, point 2, stipulates: "Consumers are parties who place their funds and/or utilize services available at Financial Services Institutions, including customers in banking, investors in the capital market, policyholders in insurance, and participants in pension funds, based on laws and regulations in the financial services sector."[31]

This provision does not regulate consumers in electronic wallets. The Financial Services Authority Regulation of the Republic of Indonesia Number 31/POJK.07/2020 concerning the Implementation of Consumer

[28] Fia Agustina Najati and Anis Mashdurohatun., The Comparative Analysis of Consumer Protection Regulations in E-Commerce Transactions in Indonesia, Singapore and Malaysia, *Law Development Journal*, Vol.6, no. 2, 2024, page. 200-213.

[29] Djafar, *Loc. Cit*.

[30] Anugerah Dian Purnama and Masitoh Indriani, Data Protection in Financial Technology Services (A Study in Indonesian Legal Perspective), *Sriwijaya Law Review*, Vol.2, No. 1, 2018, page. 82-92.

[31] Kumala Sari Nasution, and Adlin Budhiawan., Legal Protection of Insurance Policyholders of PT Aspan Medan in the Revocation of Business License by the Financial Services Authority Institution, *Journal Equity of Law and Governance*, Vol.6, no. 1, 2024, page. 103-112.

and Community Services in the Financial Services Sector provides restrictions on Financial Services Institutions, abbreviated as FSI, which are institutions that carry out activities in the banking sector, capital markets, insurance, pension funds, financing institutions, and other financial services institutions. This provision also does not explicitly mention e-wallet business actors.[32]

The existence of rules regarding the protection of personal data in e-wallets is essential; however, there are dimensions that need to be considered in the discussion of personal data, such as the interest in access to public disclosure. The protection of personal data on e-wallets is particularly important, considering that e-wallets are one of the payment systems that have gone global. Malik, Kataria and Nandal state in today's world, these digital wallets are very popular, and tomorrow, there will be a direct payment system that will be conducted through different intermediaries like mobile wallets and various companies dealing with plastic money—in other words, cashless transactions that can replace hard cash notes.[33] In relation to the protection of personal data, Bukhanevych et al. state that the protection of personal data is a fundamental element of human rights in the information society. As a basic human right, its violation endangers the security, honor, and dignity of individuals. This right is also derived from the constitutional right to privacy and the right to prohibit the collection, storage, use, and dissemination of confidential personal information.[34]

2. Legality of Personal Data Transfer Without the Consent of E-Wallet Personal Data Subjects

Privacy protection in the digital economy era, along with data and information management, requires effective security system management and oversight to minimize the occurrence of personal data theft or breaches. Hackers can sell personal data to third parties with vested interests, resulting in significant losses for the data owners. The negative impact of irresponsible parties hacking personal data is considerable. To address these issues related to privacy protection, Indonesia has established the Indonesia Data Protection System (IDPS), which aims to manage personal data and information. The IDPS consists of two important elements: a central data authority and data officers. The central data authority serves as a means to collect and secure incoming data and information from data officers. Data officers are positioned within all companies and government agencies and have the authority to manage data and privacy information from service users who have digitally

[32] Wiwik Sri Widiarty, Suwarno Suwarno, Dhaniswara K. Harjono, and Hendra Susanto., Consumer Protection Laws in Indonesian Commercial Transactions: Safeguarding Business Transactions and Consumer Rights, *Journal of Law and Sustainable Development*, Vol.12, no. 1, 2024, page. 1-16.

[33] Ritika Malik, Aarushi Kataria, and Naveen Nandal., Analysis of digital wallets for sustainability: A comparative analysis between retailers and customers, *International Journal of Management*, Vol.11, no. 7, 2020, page. 358-370.

[34] Oleksandr Bukhanevych, Igor Koropatnik, Oleksandr Zubov, Nataliia Lytvyn, and Ruslana Havrylyuk., Mechanism of administrative and legal regulation of the use of personal data by local governments, *Revista Amazonia Investiga*, Vol.10, no. 48, 2021, page. 218-227.

uploaded their data to the digital system. The Indonesia Data Protection System (IDPS) is designed to enhance data protection.

Approval for the development of payment system service activities includes the implementation of electronic wallets carried out by payment system service providers, such as banks or institutions other than banks that have obtained licenses as electronic money issuers. Parties that receive approval must comply with the provisions applicable to e-wallet operators. One of the key issues today is the security of personal data. Data security refers to the protection of data within a system aimed at countering unauthorized actions, including modification, destruction, and access by unauthorized users. There are four main aspects of data and information security: privacy/confidentiality, integrity, authentication, and availability.[35]

Privacy and confidentiality refer to efforts to protect personal data and information from individuals who do not have the right to access it. Integrity involves maintaining the accuracy of data or information and preventing unauthorized parties from altering it. Authentication is the process or method used to verify the identity of the actual owner of the personal data, often through mechanisms such as passwords, fingerprints, or facial recognition. Availability pertains to ensuring that systems and data are accessible when needed to access or interact with digital media accounts. Data security can be divided into two categories: physical security and system security. Physical security protects the physical aspects of data, including servers, terminal/client routers, and cabling. System security is designed to safeguard the operating systems and software used to access accounts on digital media platforms.[36]

Important instruments for protecting privacy in the digital economy era possess global or international characteristics. The development of legal protections for privacy in this context cannot be confined to regional efforts; instead, it must synergize with the global rule of law. This necessity arises from the nature of the media used to store personal data—cyberspace—which operates within the realm of digitization and transcends national jurisdictions, leading to cross-border implications. The principle of privacy protection for personal data that applies internationally can be found in the guidelines established by the Organization for Economic Co-operation and Development (OECD), which serves as an international institution focused on safeguarding personal data privacy.[37] In addition, international privacy protection can be summarized in European Union legislation called The General Data Protection Regulation (GDPR) which provides protection of personal data privacy against problems that carry criminal elements and regulates sanctions for violations.[38]

[35] Reni Haerani and Zaenal Muttaqin., Rancangan Implementasi Protokol S/Mime pada Layanan E-mail sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi secara Online (Studi Kasus: PT. XYZ), *JSiI (Jurnal Sistem Informasi)*, Vol.5, No. 2, 2018, page. 81-87.

[36] *Ibid.*

[37] Sinta Dewi Rosadi, and Garry Gumelar Pratama., Urgensi Perlindungandata Privasidalam Era Ekonomi Digital di Indonesia, *Veritas et Justitia*, Vol.4, no. 1, 2018, page. 88-110.

[38] *Ibid*.

The existence of legislative regulations that provide specific arrangements for the protection of privacy, which constitutes an individual's personal data, is urgent and cannot be delayed any longer. Such regulations are essential to provide legal certainty to the community and facilitate economic flows in a society that has shifted to a digitalized pattern.[39] Not only are digital platforms that accommodate merchants required to comply with data protection regulations, but merchants themselves are also obligated to maintain the personal data of their consumers. The regulations regarding the obligations of merchants in safeguarding consumer personal data are outlined in Article 58, paragraph (2) of Government Regulation Number 80 of 2019 concerning Trading Through Electronic Systems. This article states that every business actor who obtains personal data, as referred to in paragraph (1), must act as a trustee in storing and controlling personal data in accordance with the provisions of laws and regulations.[40] Consumer protection is a legal issue discussed in all countries. Yaro states that consumer protection is a matter of national, regional and global concern. This is because one of the functions of any state is protecting the citizens against the consumption of substandard products or patronizing unsatisfactory services.[41]

Personal data transfer activities are unavoidable, considering that the operation of e-wallets can be carried out across national borders. Article 20 of Law of the Republic of Indonesia Number 27 Year 2022 on the Protection of Personal Data states (1) The Controller of Personal Data must have a basis for processing Personal Data. The basis for processing Personal Data, as referred to in paragraph (1) includes:

a. explicit valid consent of the Personal Data Subject for 1 (one) or more specific purposes that has been communicated by the Personal Data Controller to the Personal Data Subject;
b. fulfillment of agreement obligations in the event that the Personal Data Subject is one of the parties or to fulfill the request of the Personal Data Subject when entering into an agreement;
c. fulfillment of legal obligations of the Personal Data Controller in accordance with the provisions of laws and regulations;
d. fulfillment of the protection of the vital interests of the Personal Data Subject;
e. the performance of tasks in the context of public interest, public service, or the exercise of the authority of the Personal Data Controller based on laws and regulations; and/or
f. Fulfillment of other legitimate interests by taking into account the

[39] Winda Fitri., The Legal Protection for Security Crowdfunding Based on Sharia Investment in MSMEs Economic Recovery, *International Journal of Law Reconstruction*, Vol.7, no. 1, 2023, page. 39-53.

[40] Dhaniswara K. Harjono., Hulman Panjaitan, Moermahadi Soerjadjanegara, Abu Hena Mostofa Kamal, and Suwarno Suwarno., Ensuring Fair Business Practices and Consumer Rights: The Role and Impact of Indonesia's Consumer Dispute Settlement Agency, *Jurnal Hukum*, Vol.40, no. 1, 2024, page.259-271.

[41] Gambo Ibrahim Yaro., Socio-cultural Inhibitions to Consumer Protection Laws in Northwestern Nigeria: A Case Study on Sokoto Metropolis, *International Journal of Business and Law Research*, Vol.8, No. 3, 2020, page. 72-78.

purposes, needs, and balance of the interests of the Personal Data Controller and the rights of the Personal Data Subject.

The provisions regarding the transfer of personal data can be seen in Articles 55 and 56 of Law No. 27 of 2022 on Personal Data Protection/ Transfer of personal data within the jurisdiction of the Republic of Indonesia. Article 55 of Law No. 27 of 2022 on Personal Data Protection states as follows:

(1) Personal Data Controller may transfer Personal Data to another Personal Data Controller within the jurisdiction of the Republic of Indonesia.
(2) Personal Data Controller who transfers Personal Data and who receives transfer of Personal Data shall be obliged to implement Personal Data Protection as referred to in this Law.

The provision in Article 56 of Law No. 27 of 2022 on Personal Data Protection does not initially require the consent of the personal data subject. The consent of the subject of personal data is only required if the provisions in paragraphs (2) and (3) are not fulfilled. This certainly weakens the protection of personal data on e-wallets, where e-wallets can be used as legal transactions across national borders. Article 56 of Law No. 27 of 2022 on Personal Data Protection states as follows:

(1) Personal Data Controller may transfer Personal Data to Personal Data Controller and/or Personal Data Processor outside the jurisdiction of the Republic of Indonesia in accordance with the provisions stipulated in this Law.
(2) In performing the transfer of Personal Data as referred to in paragraph (l), the Personal Data Controller shall be obliged to ensure that the country of domicile of the Personal Data Controller and/or Personal Data Processor receiving the transfer of Personal Data has equal or higher level of Personal Data Protection than that stipulated in this Law.
(3) In the event that the provisions as referred to in paragraph (2) are not fulfilled, the Personal Data Controller shall be obligated to ensure that there is adequate and binding Personal Data Protection.
(4) In the event that the provisions referred to in paragraphs (2) and (3) are not fulfilled, the Personal Data Controller must obtain the consent of the Personal Data Subject.
(5) Further provisions regarding the transfer of Personal Data shall be stipulated in a Government Regulation.

Legally, the validity of transferring personal data without the consent of the personal data subject can be found in the provisions of Article 56 of Law No. 27 of 2022 on Personal Data Protection. This provision permits the transfer of personal data outside the jurisdiction of the Republic of Indonesia without requiring the consent of the personal

data subject.[42] The consent of the personal data subject is only required if the provisions for data protection guarantees cannot be met. This provision undermines and weakens the principles of justice, benefit, and legal certainty regarding the protection of personal data.

D. CONCLUSION

The regulation of personal data protection for e-wallets can be examined from a comparative perspective, referencing the provisions in the United States, the United Kingdom, and Malaysia. Each state in the United States has its own laws on personal data protection. The UK has the Data Protection Act 1998 and is currently making changes to harmonize its personal data protection provisions with the General Data Protection Regulation (GDPR). In Malaysia, personal data is protected by the Personal Data Protection Act No. 709 of 2010, with implementation overseen by the Personal Data Protection Advisory Committee. The future regulatory model for the protection of personal data in e-wallets should mandate the obligation of consent from personal data subjects for the transfer of personal data, both within and outside the country. The provision in Article 56 of Law No. 27 of 2022 on Personal Data Protection, which allows the transfer of personal data outside the jurisdiction of the Republic of Indonesia without the consent of the personal data subject, undermines the protection of personal data, particularly concerning the use of e-wallets.

In the context of welfare state theory, the state has an obligation to intervene in the protection of personal data by establishing a commission to assess whether the country requesting the transfer of personal data has an adequate and equivalent personal data protection mechanism. Ensuring the security of personal data protection should not be solely the responsibility of the Personal Data Controller but should involve state authorities to guarantee justice, expediency, and legal certainty for personal data subjects. In terms of future legal reformulation, the formulation of personal data protection must focus on reconstructing rules regarding the obligation of consent, requests, and the interests of personal data subjects in data transfers across national borders. This provision can be deviated from if determined by the Minister based on the recommendation of the Personal Data Protection Commission or if the transfer is intended for legal proceedings with the permission of the Chairman of the District Court. Technical arrangements for the protection of personal data in e-wallets should be outlined in the Bank Indonesia Regulation regarding the implementation of e-wallets.

BIBLIOGRAPHY

Journals:

Alam, Md Mahmudul, Ala Eldin Awawdeh, and Azim Izzuddin Bin Muhamad., Using e-wallet for business process development: challenges and prospects in Malaysia, *Business Process Management Journal*, Vol.27, no. 4, 2021, page. 1142-1162;

[42] Edmon Makarim., Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach, *Data Protection Around the World: Privacy Laws in Action*, Vol.7, no.4, 2021, page. 127-164.

Bukhanevych, Oleksandr, Igor Koropatnik, Oleksandr Zubov, Nataliia Lytvyn, and Ruslana Havrylyuk., Mechanism of administrative and legal regulation of the use of personal data by local governments, *Revista Amazonia Investiga*, Vol.10, no. 48, 2021, page. 218-227;

Ciptarianto, Augi, and Yudo Anggoro., E-Wallet application penetration for financial inclusion in Indonesia, *International Journal of Current Science Research and Review*, Vol.5, no. 2, 2022, page. 319-332;

Fidhayanti, Dwi., Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data/Informasi Konsumen Financial Technology Pada Sektor Mobile Payment, *Jurisdictie*, Vol.11, no. 1, 2020, page. 16-47;

Fitri, Winda., The Legal Protection for Security Crowdfunding Based on Sharia Investment in MSMEs Economic Recovery, *International Journal of Law Reconstruction*, Vol.7, no. 1, 2023, page. 39-53;

Haerani, Reni and Zaenal Muttaqin., Rancangan Implementasi Protokol S/Mime pada Layanan E-mail sebagai Upaya Peningkatan Jaminan Keamanan dalam Transaksi Informasi secara Online (Studi Kasus: PT. XYZ), *JSiI (Jurnal Sistem Informasi)*, Vol.5, No. 2, 2018, page. 81-87;

Harjono, Dhaniswara K., Hulman Panjaitan, Moermahadi Soerjadjanegara, Abu Hena Mostofa Kamal, and Suwarno Suwarno., Ensuring Fair Business Practices and Consumer Rights: The Role and Impact of Indonesia's Consumer Dispute Settlement Agency, *Jurnal Hukum*, Vol.40, no. 1, 2024, page. 259-271,

Hartzog, Woodrow and Neil Richards, Privacy's Constitutional Moment and The Limits of Data Protection, *Boston College Law Review*, Vol.61, No. 5, 2020, page. 1688-1761;

Hasan, H., and C. Mustafa., The Politics of Law of Sharia Economics in Indonesia, *Lex Publica,* Vol.9, no. 1, 2022, page. 30-57;

Huang, Jie., Conflicts and tentative solutions to protecting personal data in investment arbitration, *European Journal of International Law*, Vol.32, no. 4, 2021, page. 1191-1220;

Jannah, Miftahul, F. Yudhi Priyo Amboro, and Rina Shahrullah., Personal Data Protection in Telemedicine: Comparison of Indonesian and European Union Law, *Journal of Law and Policy Transformation*, Vol.8*,* no. 2, 2023, page. 89-97;

Makarim, Edmon., Privacy and personal data protection in indonesia: the hybrid paradigm of the subjective and objective approach, *Data Protection Around the World: Privacy Laws in Action*, Vol.7, no.4, 2021, page. 127-164;

Malik, Dr Ritika, Dr Aarushi Kataria, and Dr Naveen Nandal., Analysis of digital wallets for sustainability: A comparative analysis between retailers and customers, *International Journal of Management*, Vol.11, no. 7, 2020, page. 358-370;

Mombeuil, Claudel., An exploratory investigation of factors affecting and best predicting the renewed adoption of mobile wallets, *Journal of Retailing and Consumer Services*, Vol.55, no.3, 2020, page. 102127;

Najati, Fia Agustina, and Anis Mashdurohatun., The Comparative Analysis of Consumer Protection Regulations in E-Commerce Transactions in Indonesia, Singapore and Malaysia, *Law Development Journal*, Vol.6, no. 2, 2024, page. 200-213;

Nasution, Kumala Sari, and Adlin Budhiawan., Legal Protection of Insurance Policyholders of PT Aspan Medan in the Revocation of Business License by the Financial Services Authority Institution, *Journal Equity of Law and Governance*, Vol.6, no. 1, 2024, page. 103-112;

Nathaniel, Eliezher, and I. Gede Putra Ariana., Aspek Perlindungan Hukum Internasional Data Pribadi Pengguna Layanan Jejaring Sosial dan Kewajiban Korporasi Penyedia Layanan, *Jurnal Kertha Desa*, Vol.9, no.7, 2023, page. 88-103;

Niffari, Hanifan., Perlindungan Data Pribadi Sebagai Bagian dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif dengan Peraturan Perundang-Undangan di Negara Lain), *Jurnal Yuridis*, Vol. 7, No. 1, 2020, page. 105-119;

Ni'mah, Rohmatun, and Indah Yuliana., E-Wallet: Sistem Pembayaran Dengan Prinsip Hifzul Maal, *Jurnal Ekonomi Syariah*, Vol.5, no. 2, 2020, page. 52-66;

Oluwafemi Akanfe, Rohit Valecha, and H. Raghav Rao., Design of a Compliance Index for Privacy Policies: A Study of Mobile Wallet and Remittance Services, *IEEE Transactions on Engineering Management*, Vol.70, No. 3, 2020, page. 864-876;

Purnama, Anugerah Dian and Masitoh Indriani, Data Protection in Financial Technology Services (A Study in Indonesian Legal Perspective), *Sriwijaya Law Review*, Vol.2, No. 1, 2018, page. 82-92;

Putra, Y., Comparison of personal data protection laws using narrative policy framework between indonesia, malaysia, and Japan, *Negrei Academic Journal of Law and Governance*, Vol.2, no. 2, 2022, page. 99;

Rizal, Muhammad Saiful., Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia, *Jurnal Cakrawala Hukum*, Vol.10, no. 2, 2019, page. 218-227;

Rosadi, Sinta Dewi, and Garry Gumelar Pratama., Urgensi Perlindungandata Privasidalam Era Ekonomi Digital di Indonesia, *Veritas et Justitia*, Vol.4, no. 1, 2018, page. 88-110;

Setiawati, Diana, Hary Abdul Hakim, and Fahmi Adam Hasby Yoga., Optimizing Personal Data Protection in Indonesia: Lesson Learned from China, South Korea, and Singapore, *Indonesian Comparative Law Review*, Vol.2, no. 2, 2020, page. 95-109;

Silviani, Ninne Zahara, Rina Shahriyani Shahrullah, Vanessa Riarta Atmaja, and Park Ji Hyun., Personal Data Protection in Private Sector Electronic Systems for Businesses: Indonesia vs. South Korea, *Jurnal Hukum dan Peradilan*, Vol.12, no. 3, 2023, page. 517-546;

Teng, Shasha, and Kok Wei Khong., Examining actual consumer usage of E-wallet: A case study of big data analytics, *Computers in Human Behavior*, Vol.121, no.4, 2021, page. 106778;

Theixar, Regina Natalie, and Ni Ketut Supasti Dharmawan., Tanggung Jawab Notaris Dalam Menjaga Keamanan Digitalisasi Akta, *Acta Comitas: Jurnal Hukum Kenotariatan*, Vol.6, no. 01, 2021, page. 1-15;

Tsamara, Nadiah., Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia dengan Beberapa Negara, *Jurnal Suara Hukum*, Vol. 3, No. 1, 2021, page. 53-84;

Veale, Michael, Reuben Binns, and Jef Ausloos., When data protection by design and data subject rights clash, *International Data Privacy Law*, Vol.8, no. 2, 2018, page. 105-123;

Widiarty, Wiwik Sri, Suwarno Suwarno, Dhaniswara K. Harjono, and Hendra Susanto., Consumer Protection Laws in Indonesian Commercial Transactions: Safeguarding Business Transactions and Consumer Rights, *Journal of Law and Sustainable Development*, Vol.12, no. 1, 2024, page. 1-16;

Widijowati, Dijan, and Sergiy Denysenko., Securing Consumer Rights: Ethical and Legal Measures against Advertisements that Violate Advertising Procedures, *Lex Publica*, Vol.10, no. 1, 2023, page. 28-42;

Wijayanti, Fika Arum, and Budi Santoso., The Analysis Of The Notary's Responsibilities For The Storage Of Electronic Deed Minuta, *Jurnal Hukum Volkgeist*, Vol.8, no. 1, 2023, page. 85-91;

Yaro, Gambo Ibrahim., Socio-cultural Inhibitions to Consumer Protection Laws in Northwestern Nigeria: A Case Study on Sokoto Metropolis, *International Journal of Business and Law Research*, Vol.8, No. 3, 2020, page. 72-78;

Yuniarti, Siti., Perlindungan hukum data pribadi di Indonesia, *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, Vol.1, no. 1, 2019, page. 147-154;

Internet

Djafar, Wahyudi. Hukum Perlindungan Data Pribadi di Indonesia: Lanskap, Urgensi dan Kebutuhan Pembaruan, in Public Lecture on "Tantangan Hukum dalam Era Analisis Big Data," *Program Pasca Sarjana Fakultas Hukum Universitas Gadjah Mada, 2019, http://law.ugm.ac.id/wp-content/uploads/sites/1043/2019/08/Hukum-Perlindungan-Data-Pribadi-di-Indonesia-Wahyudi-Djafar.pdf* ;

Information Commisioner Office, The Right to Erasure (The Right to be Forgotten), https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/individuals-rights/the-right-to-erasure/;

Brett, Jason. Digital Dollar and Digital Wallet Bill Surfaces in The U.S. Senate, 2020, https://www.forbes.com/sites/jasonbrett/2020/03/24/digital-dollar-and-digital-wallet-legislation-surfaces-in-the-us-senate/?sh=51220ca3866a;

Rizky, Gosta Demis., Dompet Digital Uni Eropa, Aplikasi Milik Driver di New York, dan Lainnya, 2021, https://id.techinasia.com/dompet-digital-uni-eropa-aplikasi-milik-driver-di-new-york-dan-lainnya.