

P-ISSN : 2337-9251
E-ISSN : 2957-9094

JHR

Jurnal Hukum Replik

Volume 11 No. 1 Maret 2023



Published by:
FACULTY OF LAW
UNIVERSITAS MUHAMMADIYAH TANGERANG

DAFTAR ISI

A FACILE STUDY OF THE STATUTORY CHALLENGES CONCERNING CUSTOMARY PRACTICE OF INTESTATE SUCCESSION IN NIGERIA Paul Atagamen Aidonojie, Oaihimore Idemudia Edetalehn.....	1-11
HUMAN RIGHTS AND DATA PROTECTION IN THE DIGITAL FINANCIAL ECOSYSTEM Hidayatulloh	12-28
WOMEN AND POLITICS: STRATEGIES IN OPTIMIZING WOMEN'S REPRESENTATION IN BANTEN PROVINCE LEGISLATIVE ELECTION POLITICS 2024 Muhammad Asmawi, Lathifah Sandra Devi.....	29-38
THE PRINCIPLE OF NON-DISCRIMINATION AS A FORM OF PROTECTION FOR UNDERAGE CHILDREN VICTIMS OF NARCOTICS AND PSYCHOTROPIC CRIMES Ida Ayu Rosida, Rifda Ayu Akmaliya, Sonia Amelia, Ega Permatadani, Anang Dony Irawan.....	39-52
ADOPTED CHILDREN AND HEIRS IN INHERITANCE LAW PROBLEMS: Court Judgment Number 161/Pdt.G/2021/PN.Kln and Court Judgment Number 876/Pdt.G/2019/PN.Sby Analysis Tashya Panji Nugraha, Naufal Fachri, Kelik Wardiono, Marisa Kurnianingsih	54-67
THE EFFECTIVENESS OF THE BUSINESS COMPETITION SUPERVISORY COMMISSION IN HANDLING CASES OF ALLEGED UNFAIR BUSINESS COMPETITION CONDUCTED BY PT AERO CITRA CARGO Wike Nopianti, Deny Guntara, Muhamad Abas.....	68-80
IMPLEMENTATION OF REGULATION OF THE MINISTER OF MANPOWER NUMBER 6 OF 2020 CONCERNING THE IMPLEMENTATION OF DOMESTIC APPRECIATION IN KARAWANG, WEST JAVA Listiono, Deny Guntara, Muhamad Abas	81-93
CONSUMER PROTECTION AGAINST WITHDRAWAL OF MOTOR VEHICLES BASED ON FIDUCIAN COLLATERAL Jannus Manurung, Yuniar Rahmatiar, Muhamad Abas.....	94-104
ABUSE OF AUTHORITY BY THE REGIONAL GOVERNMENT FOR THE CONSTRUCTION OF NATIONAL ROADS Ahmad Munir, Luthfie Octavian, Sugiran Try Wibowo, Bagus Teguh Santoso	105-120

**HUMAN RIGHTS AND DATA PROTECTION IN THE DIGITAL
FINANCIAL ECOSYSTEM**

Hidayatulloh

Faculty of Law, University of Miskolc, Hungary

Cím: ME ÁJK Dékáni Hivatal, Miskolc-Egyetemváros 3515

Hely: A/6-os épület Fsz. 4-18-as szoba

Telefon: 46 / 565-171, vagy 46 / 565-111/13-53

* Correspondence email: h.hidayatulloh@student.uni-miskolc.hu

Abstract

Indonesia passed Law Number 27 of 2022 concerning the Protection of Personal Data, a notable instrument in preventing privacy and data protection rights violations. This paper analyzes the relationship between human rights and personal data protection in digital financial transactions. In the findings of this paper, privacy rights and data protection rights are human rights that are interrelated with one another. Both are essential parts of protecting human honor and dignity. In matters of personal data, leakage and theft are the leading digital security issues in financial institutions, especially banks. The community hopes that Law Number 27 of 2022 can provide protection, especially the security of digital financial transactions that continue to develop in Indonesia.

Keywords: human rights, personal data protection, digital finance

INTRODUCTION

Personal data is a person's privacy who must receive protection as a form of freedom and respect for individual dignity.(van der Sloot, 2015) Everyone has the right to share or exchange personal data with others and has the right to store personal data that concerns privacy. (Zyskind & Nathan, 2015) The right to privacy through the protection of personal data is a manifestation of civil, political, spiritual, and religious freedoms for everyone.(Mutiarra & Maulana, 2020; Rianarizkiwati, 2022)

Strengthening regulations in protecting personal data strengthened due to the rapid development of information technology.(Zhang, 2018) Many people access digital media by entering their data for financial transactions, health services, education, government administration, and data exchange between individuals or institutions to social media and entertainment.(Brown et al., 2011; Williamson, 2017) Information technology collects, stores, shares, and analyzes

Jurnal Hukum Replik

Universitas Muhammadiyah Tangerang

P-ISSN: 2337-9251 E-ISSN: 2597-9094

Vol. 11 No. 1 (2023)

Submit:04-Jan-2023

Revised:05-Feb-2023

Published:30-March-2023

data from many people and includes personal data, which is the realm of individual privacy (Andrejevic, 2014). For instance, the European Union realized the urgency of modern protection for personal data due to technological developments and the invention of the internet (Shastri et al., 2019). The old regulation, the European Data Protection Directive 1995, has been obsolete due to several developments, such as financial institutions offering online banking services in 2000, Facebook becoming a public social media in 2006, and Google getting sued for scanning users' emails (Tene & Polonetsky, 2012).

Activities in the digital world with information technology have the potential to violate privacy rights by misusing the personal data of specific individuals, groups, or institutions.(Djafar, 2019; Yuniarti, 2019) The government and private parties, as collectors of personal data, can commit violations because they store a lot of personal data. Moreover, buying and selling consumer data are increasingly occurring with the aim of product marketing to embezzlement and financial transaction crimes.(Scheerens et al., 2003; Solove, 2004) The public, as data owners, is in a weak position because their data is stored by certain institutions that violate their right to privacy for financial gain (Acquisti et al., 2016).

This paper examines data protection in the digital financial ecosystem in terms of human rights (Sudarwanto & Kharisma, 2022). This study raises questions about the relationship between privacy rights and data protection rights in human rights discourse (Niffari, 2020). Besides, this study takes the example of Indonesia's data protection legal framework and relates it to data protection challenges in digital financial transactions.

METHODOLOGY

This paper uses doctrinal research methods to examine the norms and values for privacy rights and personal data protection.(Herath & Rao, 2009) Doctrinal research uses secondary data from legal scientists' scientific works and laws and regulations related to issues of human rights and the protection of

personal data, including the international covenant on human rights. In analyzing the issue of personal data protection in Indonesia, this paper examines the results of a survey by the Ministry of Communication and Information on Public Perceptions of Personal Data Protection.

Analysis and Discussion

Understanding Right to Privacy And Right to Data Protection

The word privacy is a noun which is a synonym for seclusion and secrecy. Seclusion means being separated from the observation of other parties, and secrecy means private or secret affairs. Privacy can also mean someone alone or someone's right to keep personal affairs and relationships secret, except for their free will to share personal information with others or certain groups.

The right to privacy is closely related to freedom because, in principle, every human wants individual freedom as a form of independence and to prevent interference or disturbance from other parties on himself and his private life.(Gutwirth, 2002) At least humans need four basic needs fulfilled with the right to privacy: personal autonomy by avoiding interference from other people and developing self-personality. In addition, humans want to release personal emotions in secret. Humans also need time alone for self-evaluation. Finally, humans need the right to privacy to communicate in one way of thinking (Osborne, 1969).

Protection of the right to privacy in the context of human rights refers to Article 12 of the Universal Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights (ICCPR) (O'Flaherty, 2012). Article 12 of the UDHR states that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation (Hassan, 1969). Everyone has the right to the protection of the law against such interference or attacks." Whereas Article 17 of the ICCPR states that: "(1) No one shall be subjected to arbitrary or unlawful interference

Jurnal Hukum Replik

Universitas Muhammadiyah Tangerang

P-ISSN: 2337-9251 E-ISSN: 2597-9094

Vol. 11 No. 1 (2023)

Submit:04-Jan-2023

Revised:05-Feb-2023

Published:30-March-2023

with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. (2) Everyone has the right to the protection of the law against such interference or attacks" (Diggelmann & Cleis, 2014).

Because of the importance of fulfilling the right to privacy, several countries legally regulate it in particular laws. For instance, Australia has the Privacy Act 1988, which regulates the protection of personal and sensitive information such as information on health, ethnicity, sexual preference, and trade union membership. Although in terms of sanctions and penalties, it is still less stringent than the rules for protecting personal data in the European Union (Watts & Casanovas, 2019). In addition, Canada also has a Privacy Act, which was passed in 1983. For Canada, the right to privacy as the embodiment of the principle of human dignity is the key that forms collective social values and the national legal framework. More importantly, the privacy act can regulate the right relationship and balance between the state and individuals in social life (Flaherty, 2008).

Strengthening the right to privacy is the root of the view that every individual wants to protect his personal information from access by other parties. When someone's data is leaked, such as health records, finances, and transaction preferences, due to the efforts of other people who access it secretly, it violates their right to privacy (Alfino & Mayes, 2003). However, privacy rights and data protection are considered to be unrelated because they are fundamentally different rights. This opinion received strong arguments from the separation between privacy rights and data protection in articles 7 and 8 of the Charter of Fundamental Rights of the European Union. Article 7 regulates the rights of individuals and family life, housing, and communications, while Article 8 explicitly regulates personal data protection (Gellert & Gutwirth, 2013).

In contrast, another opinion states that separating privacy and data protection rights is impossible. The main reason is that data protection is an expression of the right to privacy, so there is no violation of that right. Data

Jurnal Hukum Replik

Universitas Muhammadiyah Tangerang

P-ISSN: 2337-9251 E-ISSN: 2597-9094

Vol. 11 No. 1 (2023)

Submit:04-Jan-2023

Revised:05-Feb-2023

Published:30-March-2023

protection rights ensure that the processing of personal data does not reduce or even violate privacy rights. In addition, the processing of personal data is subject to the concept of privacy rights which protect individuals from violations of fundamental rights regarding their personal information. Moreover, the argument separating privacy and data protection rights based on the Charter of Fundamental Rights of the European Union is inappropriate because article 7 deals with the fulfillment of human rights while article 8 deals with economic matters (Kulhari, 2018).

Another argument that tries to find a middle ground for the separation of privacy and data protection in the European Union is that the relationship between privacy rights and data protection rights is contingent and unstable. Several member countries have not included personal data protection from the perspective of privacy rights. Personal data protection regulations manifest the right to access public documents, not the right to respect privacy rights. Furthermore, the configuration and protection of privacy rights and data protection rights are different. The first is a form of respect for human rights in the European Charter of Human Rights, while the second is contained in the European Union Charter and the Lisbon Agreement. The separation of the two is only conceptual. However, the two are still connected because the interpretation of data protection rights always considers the conception of privacy rights (Fuster, 2014).

In Indonesian law, the term right to privacy is not mentioned explicitly in the 1945 Constitution of the Republic of Indonesia. However, Article 28G explains that every person has the right to protection of himself/herself, family, honor, dignity, and property under his control, as well as the right to feel safe. Besides, everyone has protection from the threat of fear of doing or not doing something that is a human right. Furthermore, Law Number 39 of 1999 concerning Human Rights uses personal rights rather than privacy rights. In articles 29-32, the scope of personal rights includes:

1. everything related to oneself, family, personal property and self-esteem.
2. the right to choose to do or not do something.
3. protection of private residence from interference by other parties.
4. the freedom to communicate with anyone and guarantee the confidentiality of communications with other parties.

INDONESIAN LEGAL FRAMEWORK ON DATA PROTECTION

Indonesia passed Law Number 27 of 2022 concerning the Personal Data Protection at the House of Representatives plenary session on 20 September 2022. Personal data protection regulation is a state effort to protect human rights from misuse of personal data that is processed electronically or non-electronically. Personal data violations can cause material and non-material losses that disrupt the security and order of information in the digital era. More importantly, previously, Indonesia had many overlapping regulations related to personal data, so there needs to be a specific law that applies broadly.

Previously, Indonesia had regulated personal data protection in various laws and regulations. Provisions for data protection are included in certain articles related to the objects of the respective regulatory arrangements so that, in some cases, the rules overlap. The following include:(Firdaus, 2021)

1. Law Number 10 of 1998 concerning Banking.
2. Law Number 39 of 1999 concerning Human Rights.
3. Law Number 39 of 1999 concerning Telecommunications.
4. Law Number 14 of 2008 concerning Public Information Disclosure.
5. Law Number 36 of 2009 concerning Health.
6. Law Number 24 of 2013 concerning Population Administration.
7. Law Number 19 of 2016 concerning Information and Electronic Transactions

The personal data protection law policy is Indonesia's attempt to follow the Recommendations regarding the OECD Guidelines governing the Privacy Protection and Cross-border Flow of Personal Data on September 23, 1980. The

increasing use of personal data and the global economic risk of limiting the flow of information across borders are worrying many countries. The OECD Guidelines encourage member countries to commit to protecting privacy in the public and private sectors. The purpose of this guideline is to become a reference in formulating regulations so that there are no gaps between countries that cause legal uncertainty. The OECD updated these guidelines on 11 July 2013 due to changes in the use of personal data, as well as new approaches to privacy protection.

The Law Number 27 of 2022 applies to everyone, public bodies and international organizations that carry out legal actions within the jurisdiction of Indonesia. This Law also applies to those outside the jurisdiction of Indonesia but has legal consequences in the jurisdiction of Indonesia and is subject to the personal data of Indonesian citizens outside the jurisdiction of Indonesia.

However, this law does not apply to personal processing data in personal or household activities. For example, names and telephone numbers listed on personal cell phones are an exception under this law. This concept is similar to the Asia Pacific Economic Cooperation Privacy Framework, which excludes the process of collecting personal data by individuals for their own, family, or household needs.

Personal Data Controllers, Personal Data Processors, and Personal Data Subjects are the parties regulated in personal data protection laws. The following is an explanation:

1. Data Controller is any person, public body or international organization acting individually or jointly in determining the purpose and exercising control over personal processing data.
2. Data Processor is any person, public body or international organization acting individually or jointly in processing personal data on behalf of the Personal Data Controller.
3. Data subject is individual to whom personal data is attached.

The principles of personal data protection based on Law Number 27 of 2022:

- a. Protection. Each data processing protects personal data, and there is no data misuse.
- b. Legal certainty. Every data processing is subject to and complies with the rule of law and obtains legal recognition inside and outside the court.
- c. Public interest. Personal data protection must pay attention to public interests such as state administration, security, and national defense.
- d. Expediency. The purpose of regulating personal data protection is for the benefit of the national interest and public welfare.
- e. Circumspection. Every party processing personal data must apply the precautionary principle and prevent potential losses.
- f. Balance. Protection of personal data strikes a balance between rights to personal data and legitimate state rights based on the public interest.
- g. Accountability. All parties involved in the processing and monitoring personal data serve responsibly to ensure a balance between the rights and obligations of the parties.
- h. Secrecy. Personal data gets protection from unauthorized parties and unauthorized processing activities.

Personal data is divided into general personal data and specific personal data. Personal data is a full name, gender, nationality, religion, marital status, and personal data combined to identify an individual, such as cell phone number and IP address. Meanwhile, specific personal data are health data and information, biometric data, genetic data, criminal records, child data, personal financial data, and other data according to the provisions of the law.

In protecting privacy rights, Indonesian data protection law provides:

- a. the right for every personal data owner to obtain information about the clarity of identity,
- b. the basis of legal interest,
- c. the purpose of requesting and using personal data, and

d. accountability of the party requesting personal data.

In addition, each individual has the right to request access and obtain a copy of his data. Everyone can complete and update if there is a shortage or irregularity in data. Moreover, everyone can request the deletion of personal data submitted to the personal data manager. If there is a violation in the processing of personal data, the data owner can sue and receive compensation from the personal data processor.

However, privacy rights related to personal data may be waived in the interests of national defense and security, the interests of the law enforcement process, the public interest in the context of administering the state, the interests of supervising the financial services sector, monetary, payment systems, and financial system stability in the context of administering the state, and interests of statistics and scientific research. All such exceptions can only occur due to the implementation of the law.

Controllers and Processors of personal data, such as persons, public bodies or international organizations, have obligations to the personal data they maintain. The basis for the processing of personal data is the explicit valid consent of the personal data subject, such as through written or recorded consent which has the same legal force. Approval can be submitted manually or electronically. Agreements must be distinguishable, made in a format that is easy to understand and accessible, and use simple and clear language. For children, processing their data is mandatory with the consent of their parents or guardians according to the law. When a person consents to process personal data, the personal data controller is obliged to provide information regarding legality, purpose, type and relevance, document retention period, information details, time and rights of the personal data subject.

The personal data controller must protect and ensure the security of the personal data it processes. They are required to develop and implement operational techniques for data processing disturbances and determine the level of

security by considering risks. In addition, they must maintain the confidentiality of personal data properly by supervising each party involved in the data processing. In order to prevent unauthorized access by other parties, they must use a security system that is safe, reliable, and responsible. They are also obliged to delete personal data when it is no longer needed, withdraw consent or withdrawal by the personal data subject, or unlawful data processing.

Personal data protection law has regulated administrative sanctions and criminal provisions to prevent violations and criminal acts. Controllers and processors of personal data may receive administrative sanctions if they violate the provisions on personal data processing. For instance, written warnings, temporary suspension of personal data processing activities, deletion or destruction of data, or administrative fines of up to two per cent of annual income or annual receipts of variable violations.

Concerning criminal provisions, anyone who deliberately and unlawfully obtains or collects personal data belonging to other people for personal gain and harm is subject to a maximum legal threat of five years in prison and a maximum fine of five billion rupiahs. In addition, anyone who deliberately creates false personal data or falsifies personal data to benefit himself or harm others is subject to a maximum imprisonment of six years or a maximum fine of six billion rupiahs.

Criminal sanctions do not only apply to people but also to corporations. Any corporation that obtains or collects personal data for its own and other people's benefit creates false data or falsifies personal data and is subject to criminal penalties of fines. Fines can be imposed on administrators, controllers, givers of orders, beneficial owners or corporations. Fines are a maximum of ten times the maximum fines that are threatened. Even additional penalties can be imposed on corporations in the form of:

- a. confiscation of wealth or profits derived from the proceeds of crime,
- b. freezing of part or all the business,
- c. permanent prohibition of certain actions,

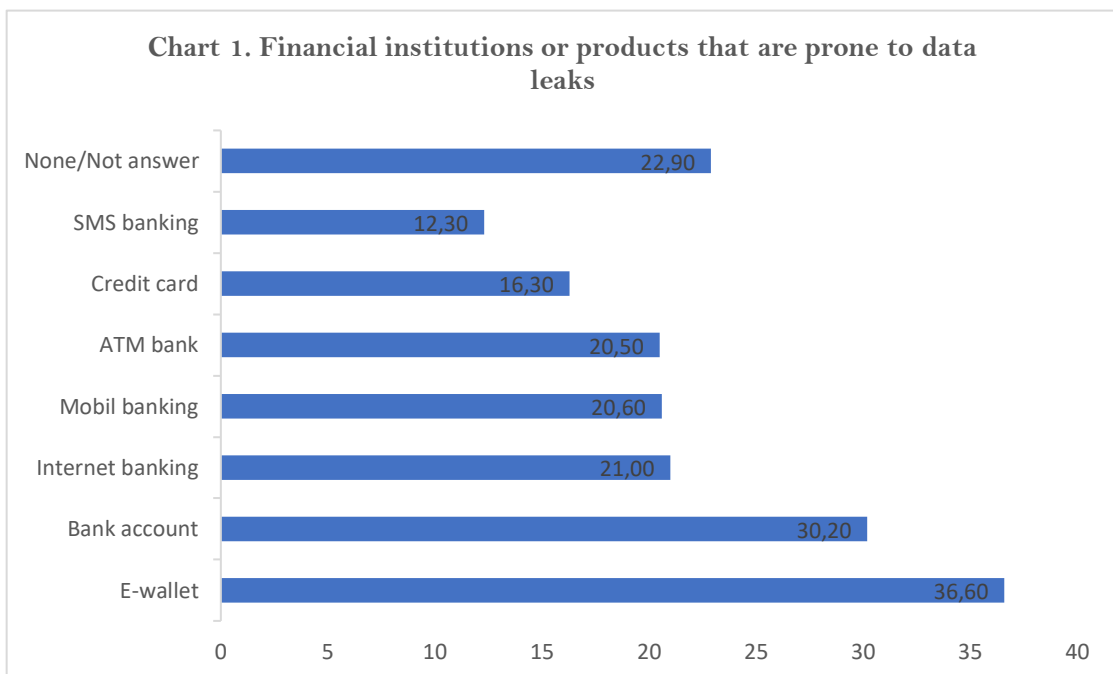
- d. closure of all or part of the place of business or activity,
- e. carry out obligations that have been neglected,
- f. compensation payment,
- g. license revocation, or
- h. corporation dissolution.

THE URGENCY OF DATA PROTECTION FOR THE DIGITAL FINANCIAL ECOSYSTEM

The sophistication and speed of information technology encourage people to interact more broadly, including in global financial transactions. However, the potential for leakage and misuse of personal data will continue to expand in line with the broader reach of public finance transactions. In the case of Indonesia, for example, two main issues are of concern to the public regarding the security of their data. First, many individuals and community groups have complained about cases of misuse of personal data that government agencies and private companies should protect. Second, people complain about personal data leakages in the financial industry, such as banking, insurance, and other financial institutions (Apriyanti, 2020). The financial industry that stores the personal data of its customers can experience data theft by hackers to be traded to other parties.

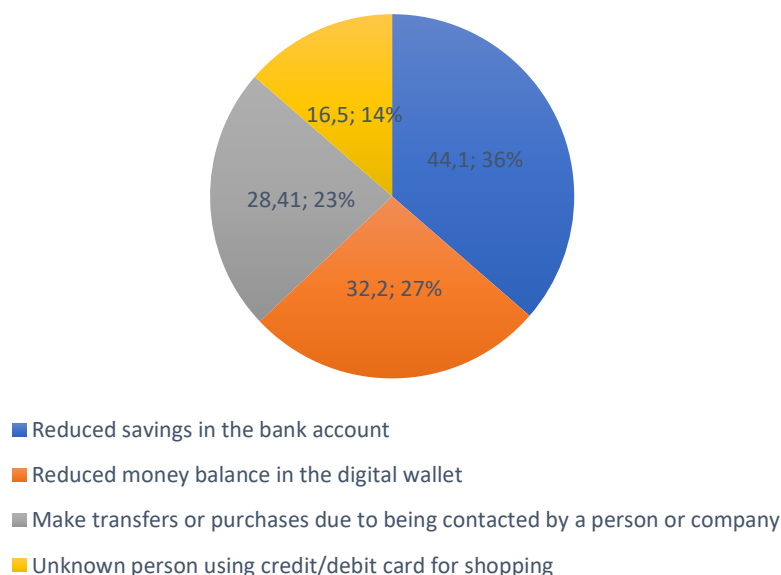
In an information security system, incidents of accessing, snooping, and theft of personal data by third parties are called data breaches. In an information security system, incidents of accessing, snooping, and theft of personal data by third parties are called data breaches. Based on data from cybersecurity company Surfshark, Indonesia ranks third in the world for data leaks after Russia and France. Surfshark recorded 12.74 million accounts that experienced data leaks during the third quarter of 2022. Under Indonesia, there are several large countries, such as the United States, China, Taiwan, Brazil, India, Colombia, and Nigeria.

Based on a national survey conducted by the Indonesian Ministry of Communication and Informatics in 2021, most respondents considered that electronic wallets and bank accounts are financial products that are most vulnerable to data leaks. Internet banking and mobile banking rank third and fourth, while SMS banking ranks lowest. As a result of personal data leaks, most respondents experienced reduced savings in bank accounts or balances in digital wallets. Another disadvantage is making a transfer or purchasing something



because someone else contacted it, and credit/debit card cases were spent by someone else.

Chart 2. Impact of financial data leaks



To increase protection for consumers of financial services, particularly personal data protection, the Indonesian Financial Services Authority revised POJK Number 1 of 2013 with POJK Number 6 of 2022 concerning Consumer and Community Protection. Protection of consumer assets, privacy, and data apply the principle of certainty of procedures, mechanisms, and security systems, protection, and confidentiality of consumer financial assets. In addition, OJK emphasizes that financial service businesses use personal consumer data following the interests and purposes approved by consumers and subject to the law.

More explicitly, Article 11 POJK Number 6 of 2022 prohibits financial service actors from providing personal data and information about consumers to other parties. In agreements or financial transactions, consumer consent is mandatory regarding providing personal data and information in specific financial products or services. In addition, financial institutions may not use the personal data and information of consumers who have terminated the agreement on products or services or potential customers who have canceled or been refused to use the product or service.

CONCLUSION

The framework for protecting personal data is firmly rooted in protecting the right to privacy as a human rights principle. Even though there are differences between privacy and data protection rights, both are related as part of respecting human dignity. Various human rights instruments, such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, and the Charter of Fundamental Rights of the European Union, regulate privacy rights and data protection rights as guidelines for many countries in the world.

Indonesia introduced a personal data protection law at the end of 2022 as a special law that accommodates privacy rights and data protection rights as a strengthening of human rights and preventing previous overlapping regulations. In particular, many personal data breaches and crimes occur in digital finance. Therefore, in addition to the personal data protection law, the Indonesian Financial Services Authority issued a consumer protection POJK to prevent the misuse of personal data in the financial services sector.

REFERENCES

- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, 54(2), 442–492.
- Alfino, M., & Mayes, G. R. (2003). Reconstructing the right to privacy. *Social Theory and Practice*, 29(1), 1–18.
- Andrejevic, M. (2014). Big data, big questions | the big data divide. *International Journal of Communication*, 8, 17.
- Apriyanti, I. (2020). The Urgency of Establishing Personal Data Protection Act and Financial Technology Act in Digital Era in order to Protect and

Jurnal Hukum Replik

Universitas Muhammadiyah Tangerang

P-ISSN: 2337-9251 E-ISSN: 2597-9094

Vol. 11 No. 1 (2023)

Submit:04-Jan-2023

Revised:05-Feb-2023

Published:30-March-2023

- Control the Privacy in Indonesia. *3rd International Conference on Law and Governance (ICLAVE 2019)*, 345–356.
- Brown, B., Chui, M., & Manyika, J. (2011). Are you ready for the era of ‘big data’. *McKinsey Quarterly*, 4(1), 24–35.
- Diggelmann, O., & Cleis, M. N. (2014). How the right to privacy became a human right. *Human Rights Law Review*, 14(3), 441–458.
- Djafar, W. (2019). Hukum perlindungan data pribadi di indonesia: Lanskap, urgensi dan kebutuhan pembaruan. *Seminar Hukum Dalam Era Analisis Big Data, Program Pasca Sarjana Fakultas Hukum UGM*, 26.
- Firdaus, M. (2021). *A Review of Personal Data Protection Law in Indonesia*.
- Flaherty, D. H. (2008). *Reflections on Reform of the Federal Privacy Act*. Office of the Privacy Commissioner of Canada.
- Fuster, G. G. (2014). *The emergence of personal data protection as a fundamental right of the EU* (Vol. 16). Springer Science & Business.
- Gellert, R., & Gutwirth, S. (2013). The legal construction of privacy and data protection. *Computer Law & Security Review*, 29(5), 522–530.
- Gutwirth, S. (2002). *Privacy and the information age*. Rowman & Littlefield.
- Hassan, P. (1969). International Covenants on Human Rights: An Approach to Interpretation, The. *Buff. L. Rev.*, 19, 35.
- Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, 47(2), 154–165.
- Kulhari, S. (2018). *Building-Blocks of a Data Protection Revolution*. Nomos Verlagsgesellschaft mbH & Co. KG.
- Mutiara, U., & Maulana, R. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi. *Indonesian Journal of Law and Policy Studies*, 1(1), 42–54.
- Niffari, H. (2020). Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi (Suatu Tinjauan Komparatif

Jurnal Hukum Replik

Universitas Muhammadiyah Tangerang

P-ISSN: 2337-9251 E-ISSN: 2597-9094

Vol. 11 No. 1 (2023)

Submit:04-Jan-2023

Revised:05-Feb-2023

Published:30-March-2023

- Dengan Peraturan Perundang-Undangan Di Negara Lain). *Jurnal Yuridis*, 7(1), 105–119.
- O’Flaherty, M. (2012). Freedom of expression: Article 19 of the international covenant on civil and political rights and the human rights committee’s general comment no 34. *Human Rights Law Review*, 12(4), 627–654.
- Osborne, D. E. (1969). Part V: Judicial Protection of Water Resources: Private Action, the Public Trust Doctrine, and Administrative Review. *Tex. L. Rev.*, 48, 1169.
- Rianarizkiwati, N. (2022). Ius Constituendum Hak Atas Pelindungan Data Pribadi: Suatu Perspektif Hak Asasi Manusia. *Jurnal Hukum Sasana*, 8(2), 324–341.
- Scheerens, J., Al-Jauhari, A., & Syahid, A. (2003). *Peningkatan mutu sekolah*. Logos.
- Shastri, S., Wasserman, M., & Chidambaram, V. (2019). The seven sins of personal-data processing systems under GDPR. *ArXiv Preprint ArXiv:1903.09305*.
- Solove, D. J. (2004). *The digital person: Technology and privacy in the information age* (Vol. 1). NyU Press.
- Sudarwanto, A. S., & Kharisma, D. B. B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. *Journal of Financial Crime*, 29(4), 1443–1457.
- Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw. J. Tech. & Intell. Prop.*, 11, xxvii.
- van der Sloot, B. (2015). Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system. *Computer Law & Security Review*, 31(1), 26–45.
- Watts, D., & Casanovas, P. (2019). Privacy and Data Protection in Australia: A critical overview. *W3C Workshop on Privacy and Linked Data*.
- Williamson, B. (2017). Big data in education: The digital future of learning, policy and practice. *Big Data in Education*, 1–256.

Jurnal Hukum Replik

Universitas Muhammadiyah Tangerang


P-ISSN: 2337-9251 E-ISSN: 2597-9094

Vol. 11 No. 1 (2023)

Submit:04-Jan-2023

Revised:05-Feb-2023

Published:30-March-2023

- 
- Yuniarti, S. (2019). Perlindungan hukum data pribadi di Indonesia. *Business Economic, Communication, and Social Sciences Journal (BECOSS)*, 1(1), 147–154.
- Zhang, D. (2018). Big data security and privacy protection. *8th International Conference on Management and Computer Science (ICMCS 2018)*, 275–278.
- Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, 180–184.