LEGAL SPIRIT

E-ISSN : 1978-2608 Volume 8, (2), 2024

http://publishing-widyagama.ac.id/ejournal-v2/index.php/jhls/

Guardians of Privacy: Unraveling the Tapestry of Personal Data Protection in Indonesia and France

Merizqa Ariani[1], FL. Yudhi Priyo Amboro[2], Nurlaily[3]

[1] Faculty of Law, Unversitas Internasional Batam, Indonesia, 2152058.merizqa@uib.edu
[2] Faculty of Law, Unversitas Internasional Batam, Indonesia
[3] Faculty of Law, Unversitas Internasional Batam, Indonesia

ABSTRACT

The rapid advancement of technology has facilitated easier access to information but has concurrently heightened the risks associated with the security of personal data. This has raised concerns about individual privacy, prompting the enactment of regulations for the protection of personal data. Legal enforcement becomes crucial to ensure proper treatment of personal data. Indonesia responded to the increasing cases of data breaches by enacting the Personal Data Protection Act in 2022. However, incidents of data leaks persist. France boasts a well-established data protection law, notably the General Data Protection Regulation (GDPR), which provides comprehensive guidelines for the management of personal data. There are similarities and differences in the approaches of the two countries. Both emphasize principles such as fairness, transparency, and responsibility. However, France highlights openness and integrity, while Indonesia places a greater focus on fairness and responsibility. Individual rights take center stage in both regulatory frameworks, with an emphasis on access, correction, and deletion of data. France introduces the rights to protest and data portability to afford individuals greater control over their personal data. Sanctions and legal enforcement are also crucial in safeguarding personal data. Both countries impose sanctions, though there are variations in implementation and enforcement. This research aims to provide a better understanding of the differences and similarities in the frameworks for personal data protection between Indonesia and France, with the goal of strengthening data protection and enhancing public awareness.

Keywords	*Personal Data Protection; Law Enforcement; Legal Comparison*
Cite This Paper	Ariani, M., Amboro, F. Y., & Nurlaily. (2024). Guardians of Privacy: Unraveling the Tapestry of Personal Data Protection in Indonesia and France. *Legal Spirit, 8*(2).
Manuscript History: *Received:* 2024-01-26 *Accepted:* 2024-07-17 *Corresponding Author:* Merizqa Ariani, 2152058.merizqa@uib.edu	Legal Spirit is *Licensed under a Creative Commons Attribution-ShareAlike 4.0 International License* **Indexed:** **Layout Version:** V8.2024

INTRODUCTION

The rapid development of current technology has enabled everyone to access anything with just a touch on their favorite gadgets, even without traveling the world, as individuals can see what is beyond their reach right in the palm of their hands.[1] However,

[1] Disemadi, H. S., & Budi, H. S. (2023). Enhancing Trade Secret Protection amidst E-commerce Advancements: Navigating the Cybersecurity Conundrum. *Jurnal Wawasan Yuridika*, *7*(1), 21-45.

this technological advancement is accompanied by several challenges, one of which revolves around personal data.[2] The information disclosed through electronic media is invaluable, as it is private and carries risks that may lead to problems if the data falls into the wrong hands, potentially being misused by irresponsible parties[3]. This phenomenon raises concerns about personal data privacy, prompting the development of regulations aimed at safeguarding individual privacy rights.[4] The enforcement of personal data protection laws plays a crucial role in ensuring that someone's personal information is treated properly and securely.[5] Protecting individual privacy is an obligation to maintain the confidentiality of personal data, as it is included in the individual's right to privacy.[6] Failure to safeguard one's privacy may result in consequences different from physical harm, as others can freely interfere with individual privacy and misuse it[7]. The leakage of personal data can trigger various disruptive actions such as spam attacks through email and SMS, as well as other harmful activities.[8] Moreover, the exposed data can be a source of various detrimental cybercrimes against consumers. In practice, cybercriminals often use phishing methods, a form of fraud that manipulates victims into indirectly providing all the desired information to the criminal[9].

Given the increasing number of cases, Indonesia has enacted legislation concerning personal data, namely Law No. 27 of 2022 on Personal Data Protection (PDP Law), which came into effect on October 17, 2022. This law is expected to protect the Indonesian community, as data breaches have become a serious and frequent problem. One notable data breach case occurred at PT. Tokopedia in 2020, where the personal data of 91 million Tokopedia users was successfully hacked. This data breach had widespread implications, leading the Consumer Community of Indonesia to take legal action by filing a lawsuit against PT. Tokopedia and the Minister of Communication and Information. The lawsuit was filed because PT. Tokopedia was deemed negligent in securing user data. The compromised data included crucial information such as user IDs, email addresses, full names, addresses, phone numbers, birth dates, gender, and encrypted passwords. This information could be exploited by irresponsible parties for crimes like fraud, extortion, and identity theft. On March 21, 2020, a hacker known as whysodank successfully sold the data of 91 million users for USD 5000 or approximately 75,000,000 Indonesian Rupiah on the dark web's empire market[10]. This incident highlights the significant impact of data breaches, not only on individuals but also on society and the economy as a whole. Therefore, it is crucial for everyone to raise awareness of data security and take measures to protect their personal data. Even after the enactment of the law, some cases of personal data breaches persist, as exemplified by Bjorka leaking the personal information of around 44 million MyPertamina application users, which was then sold for Rp392 million in Bitcoin. This incident was exposed through Bjorka's latest post titled 'MYPERTAMINA INDONESIA 44 MILLION' on the BreachForums website on

[2] Anjawai, N. B., Amboro, F. Y. P., & Hutauruk, R. H. (2022). Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*, *4*(2), 207-218.

[3] Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, 20(2), 369-384.. Hal. 371

[4] Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, *5*(2), 177-199.

[5] Amboro, F. Y. P., & Puspita, V. (2021, March). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia). In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences* (Vol. 1, No. 1, pp. 415-427).

[6] Afnesia, U., & Ayunda, R. (2021). Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(3), 1035-1044.

[7] Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, 5(2), 206-221.

[8] Stevani, W., & Sudirman, L. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. *Journal of Judicial Review*, *23*(2), 197-216.

[9] Wibowo, M. H., & Fatimah, N. (2017). Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime. *JOEICT (Jurnal of Education and Information Communication Technology),* 1(1), 1-2.Hal. 2

[10] Sylfia, A., Amrullah, M. F., & Djaja, H. (2021). Tanggungjawab Yuridis PT. Tokopedia atas Kebocoran Data Pribadi dan Privasi Konsumen Dalam Transaksi Online. *Bhirawa Law Journal*, 2(1), 21-27.

Thursday (10/11) at 02:31 AM. MyPertamina is a digital financial services platform developed by Pertamina, integrated with the LinkAja application for non-cash payments at Pertamina gas stations. The leaked data consisted of a 6GB compressed file and a 30GB uncompressed file, totaling 44,237,264 data entries[11]. From the aforementioned cases, it can be concluded that user data breaches pose a serious threat. Therefore, it is essential to enhance both preventive and punitive measures to prevent data breaches and safeguard the security of users' personal data[12]. The 1945 Constitution explicitly states that human rights are protected, and implicit provisions related to data protection can be found in Article 28F and 28G(1), which are linked to freedom to store information and the protection of data and the information accompanying it. This serves as the foundation for all legal regulations governing privacy as a human right, in addition to legal certainty (a requirement for legal rules), including the Personal Data Protection Law.

In 2022, Indonesia took a significant step forward in addressing the challenges of personal data security by enacting Law Number 27 of 2022 on Personal Data Protection (PDPA). This legislation serves as the primary foundation for safeguarding individual privacy in Indonesia, providing clear definitions of personal data and establishing key principles to be followed by those managing such data.[13] These principles include notions of fairness, transparency, and responsibility in data management.[14] The PDPA represents a concrete measure to protect individual privacy in an era where digital information exchange is increasingly pervasive. A pivotal concern addressed by the PDPA is the rising incidence of detrimental data breaches affecting users, with high-profile cases like the Tokopedia user data leak serving as a crucial impetus for its formulation. The aim of the PDPA is to fortify protection and ensure the rights of individuals concerning their personal data. France stands as a long-time proponent of personal data protection regulations, primarily governed by the French Data Protection Act (Loi Informatique et Libertés) and the General Data Protection Regulation (GDPR) applicable in European Union member states. The privacy supervisory authority in France, known as the Commission nationale de l'informatique et des libertés (CNIL), holds the responsibility for enforcing data protection laws in the country. CNIL possesses the authority to conduct investigations, impose fines, and provide guidance on compliance with data protection regulations. As a EU member state, France is obligated to adhere to the GDPR, having incorporated its provisions into national law by amending the French Data Protection Act.

Research related to personal data protection has been previously conducted, such as the study examining the Importance of Personal Data Protection Laws in Indonesia: A Comparative Analysis with English and Malaysian Laws[15], the Legal Protection of Personal Data: A Comparative Analysis between Indonesia and Norway[16], a Comparative Analysis of Legal Protection Regarding Personal Data in Indonesia and Germany[17], a Comparison of Personal Data Protection Laws in Indonesia and Malaysia[18], a Comparative Study on

[11] CNN Indonesia.com. 2022. "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah", (https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2, diakses 1 Juni 2023).

[12] Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law Review,* 9(1).

[13] Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review,* 5(1), 39-57.

[14] Purnama, T. D., & Alhakim, A. (2021). Pentingnya Uu Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia. *Jurnal Komunitas Yustisia*, 4(3), 1056-1064.

[15] Sautunnida, L. *Op.cit*

[16] Amboro, F. Y. P., & Puspita, V. (2021, March). *Op.Cit.*

[17] Anjawai, N. B., Amboro, F. Y. P., & Hutauruk, R. H. (2022). *Op.Cit.*

[18] Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum,* 10(2), 218-227.

Personal Data Protection in Indonesia and the European Union[19], Data Protection Officers in the Ecosystem of Personal Data Protection: Indonesia, the European Union, and Singapore[20], and a Comparison of Privacy Protection Rules on Personal Data between Indonesia and Several Countries[21]. Unlike previous research, the focus of this study is to discern differences and similarities in legal approaches, regulatory frameworks, and enforcement practices in both countries. This aims to provide a better understanding of personal data protection efforts in each nation and identify strengths and weaknesses within the existing legal frameworks. Theoretically, this research serves as a valuable reference on legal comparisons regarding personal data protection, while practically enhancing public understanding of personal data protection.

METHOD

In this study, the author employs a normative research design incorporating various approaches in legal writing. According to Mahmud Marzuki, five distinct approaches are utilized in legal research writing: the statutory approach, case approach, historical approach, comparative approach, and conceptual approach[22]. The emphasis of this legal research is predominantly on the use of secondary data. To add depth and diversity to the analysis, primary data is also applied as a primary supporting element. The nature of this research is descriptive, encompassing two vital types of data.[23] Firstly, referred to as secondary data, which constitutes pre-existing information. Secondly, referred to as primary data, obtained directly from the original source. Subsequently, both types of data are meticulously elucidated and conclusions are drawn using deductive reasoning. In this deductive process, the research initiates by detailing general propositions whose truth is known or believed, culminating in the discovery of new, more specific knowledge.[24] This approach facilitates a deeper exploration of each data aspect, ensuring a more profound analysis and yielding a more detailed and specific understanding of the subject matter in this legal research.

RESULT AND DISCUSSIONS

Violations may arise as a consequence of irresponsible handling of personal data, such as the exchange of someone's personal data without clear consent.[25] The safeguarding of personal data has emerged as one of the most critical issues in recent times, particularly with the heightened usage of digital platforms. Therefore, ensuring the security of personal data stands as a pivotal rationale for enhancing personal data protection[26].

Regulation on Personal Data Protection in Indonesia

[19] Ramadhani, S. A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis*, *3*(1), 73-84.

[20] Yuniarti, S. (2022). Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura. *Business Economic, Communication, and Social Sciences Journal (BECOSS),* 4(2), 111-120.

[21] Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, *3*(1), 53-84.

[22] Marzuki, M. (2017). *Penelitian Hukum: Edisi Revisi*. Prenada Media. Hal. 60

[23] Sudirman, L., Situmeang, A., & Fiona, F. (2023). Enhancing Geographical Indications Product Protection: A Comparative Study of Indonesia and India. *Journal of Judicial Review*, *25*(2), 287-312.

[24] Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, *24*(2), 289-304.

[25] Disemadi, H. S., & Prasetyo, D. (2021). Tanda Tangan Elektronik pada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia. *Wajah Hukum*, *5*(1), 13-20.

[26] Mardiana, N., & Meilan, A. (2023). Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia,* 5(1), 16-23. Hal. 18

The enactment of Law Number 27 of 2022 on Personal Data Protection (PDPL) serves as the primary foundation for safeguarding individual privacy in Indonesia. This law provides a clear definition of personal data and establishes key principles that must be adhered to by those managing personal data. These principles include fairness, transparency, and responsibility in data management[27]. Additionally, the law imposes obligations on data controllers, requiring them to have a strong legal basis for personal data management, provide clear information to data owners, and involve data protection authorities in the processing process[28]. Protection of individual rights takes center stage in this legislation. Individuals have the right to access, correct, and delete their personal data managed by others, granting them greater control over their personal information[29]. To ensure compliance, the law introduces administrative and criminal sanctions for violations. Data protection authorities play a crucial role in supervision and law enforcement, imposing sanctions commensurate with the level of violation[30]. While the PDPL establishes a robust legal framework for protecting personal data, challenges persist in its implementation. Challenges include non-compliance from businesses, lack of public awareness regarding their rights related to personal data, and evolving cybersecurity threats. Addressing these challenges requires close collaboration between the government, private sector, and civil society. Proposed measures include: 1) Extensive public education to raise awareness about the importance of personal data protection; 2) Training for businesses to enhance their understanding of PDPL compliance; 3) Strengthening the capacity of law enforcement agencies to enforce the PDPL.

The Personal Data Protection Law (PDPL), officially ratified in 2022, marks a significant milestone in the effort to protect personal data in Indonesia.[31] However, it is crucial to recognize that the PDPL is not the ultimate pinnacle but a foundation requiring periodic revisions to stay aligned with technological advancements and emerging challenges. Planned and scheduled revisions of the PDPL are advisable due to two main factors. Firstly, rapid technological advancements pose new risks to the security of personal data, necessitating continuous updates to address and mitigate these risks.[32] Secondly, new challenges, such as sophisticated cybersecurity threats, highlight the need to fortify the PDPL to remain effective in safeguarding personal data. The revision process should involve various stakeholders, including the government, private sector, and civil society, ensuring holistic representation and accurate adjustments to the needs and aspirations of all stakeholders. Transparency and accountability in the revision process are crucial aspects to maintain public trust. The PDPL brings several benefits to Indonesia.[33] Besides reinforcing the protection of its citizens' personal data, this revision creates a legal foundation adaptable to the evolving digital environment. Citizens gain additional confidence in the security and privacy of their data, strengthening Indonesia's position in addressing global challenges related to personal data protection. With a commitment to continually align regulations with the dynamics of the digital world, the PDPL revision reflects Indonesia's determination to provide optimal protection for the personal data of every individual.

Regulatory Overview of Personal Data Protection in France

[27] Undang-Undang Nomor 27 Tahun 2022 Pasal 1 ayat (1).
[28] Undang-Undang Nomor 27 Tahun 2022 Pasal 7
[29] Undang-Undang Nomor 27 Tahun 2022 Pasal 12
[30] Undang-Undang Nomor 27 Tahun 2022 Pasal 42
[31] Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?. *Sang Sewagati Journal*, *1*(2), 66-90.
[32] Sudirman, L., Disemadi, H. S., & Aninda, A. M. (2023). Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective. *JED (Jurnal Etika Demokrasi)*, *8*(4), 497-510.
[33] Hartono, J., AW, A. M., Nugraha, X., & Felicia, S. A. (2023). Failing to Protect Personal Data: Key Aspects of Electronic System Operators' Agreements. *Barelang Journal of Legal Studies*, *1*(1), 31-55.

France adheres to the General Data Protection Regulation (GDPR), a regulation implemented by the European Union (EU) that sets guidelines on the collection, processing, and storage of personal data of individuals within the EU. Adopted in 2016, the GDPR came into effect in May 2018. As a member state of the EU, France is obligated to comply with the GDPR and has incorporated its provisions into its national laws. The French Data Protection Law (Loi Informatique et Libertés) has been modified to align with the requirements of the GDPR. This action ensures that individuals in France receive the same level of protection for their personal data as outlined in the GDPR. The data protection authority in France, known as the Commission nationale de l'informatique et des libertés (CNIL), is responsible for enforcing data protection regulations in the country. In France, data protection laws are primarily governed by the French Data Protection Law (Loi Informatique et Libertés) and the General Data Protection Regulation (GDPR), which applies to all EU member states. The French Data Protection Law, first introduced in 1978, has undergone revisions to align with GDPR requirements. This law establishes principles and rules for the processing of personal data in France, including definitions of personal data, individual rights as data subjects, and the obligations of data controllers and processors.

Within the framework of the French Data Protection Law, individuals have rights such as access and correction of their personal data, the right to object to data processing, and the right to erasure of data. Data controllers must inform individuals of the purpose and legal basis for data processing and obtain their consent when required. Additionally, they are obligated to implement appropriate security measures to protect personal data from unauthorized access, loss, or disclosure. The CNIL, as the data protection authority in France, is responsible for enforcing data protection laws. CNIL has the authority to conduct investigations, impose fines as sanctions, and provide guidance on compliance with data protection regulations. It is crucial to note that as a member of the European Union, France is also subject to the GDPR. The GDPR establishes comprehensive and uniform data protection rules across the EU, superseding national laws in cases of non-compliance. Overall, data protection laws in France aim to safeguard the privacy and rights of individuals related to the processing of their personal data, while providing a framework for organizations to responsibly and securely manage data.

Similarities and Differences in the Legal Framework for Personal Data Protection between Indonesia and France

a. Definition of Personal Data

In Indonesia, the definition of personal data is governed by the Personal Data Protection Law in Article 1(1): Meanwhile, France establishes its definition of personal data under GDPR Article 4(1): “Personal Data refers to any information related to an identified or identifiable individual ('data subject'). An identifiable individual includes a person who can be identified directly or indirectly, particularly by reference to an identifier such as a name, identification number, location data, online identifier, or one or more specific factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that individual[34].

b. Law and Institutions

Indonesia enacted the Personal Data Protection Law (PDP Law) in 2022, outlining principles for the safeguarding of personal data in accordance with international norms. The Personal Data Protection Authority (PDPA) was established as the governing body responsible for enforcing the PDP Law in the country. Meanwhile, in France, the Loi Informatique et Libertés (LIL) was enacted in 1978 and has undergone several revisions, including in 2004 and 2018. Serving as the legal framework in France governing the use of personal data by the private sector, the LIL has evolved over the years. At the European

[34] General Data Protection Regulation article 4(1)

Union level, the General Data Protection Regulation (GDPR) serves as the overarching law applicable across the region, including France, setting higher standards for the protection of personal data compared to those stipulated by the LIL. The Commission Nationale de l'Informatique et des Libertés (CNIL) functions as the personal data protection authority in France, tasked with overseeing and enforcing compliance with data protection regulations, including the GDPR. Consequently, both Indonesia and France have established legal frameworks and authorities to regulate the management of personal data, ensuring protection in line with national and international standards.

c. Principles of Data Protection (Similarities and Differences)

Both of these countries highlight the same fundamental principles regarding data protection. In Indonesia, these principles include: 1) Justice: Personal data must be protected fairly and equally, without discrimination; 2) Transparency: Individuals must be informed about how their personal data will be used; and 3) Responsibility: Companies must be accountable for their compliance with data protection regulations[35]. The key differences between these two countries lie in the emphasis on different principles. In Indonesia, the primary principles upheld are justice and responsibility. Meanwhile, in France, openness and integrity also play a crucial role, especially in line with European Union regulations: 1. Justice: This principle emphasizes that every individual should have equal rights in protecting their personal data, indicating that the protection of personal data should not vary based on race, religion, gender, or other characteristics. 2. Transparency: This principle focuses on the obligation to provide information to individuals about how their personal data will be used. It includes the company's responsibility to provide clear and understandable information to individuals about the processes of collecting, using, and sharing their personal data. 3. Responsibility: This principle emphasizes that companies must be responsible for their compliance with data protection regulations. This means that companies are expected to take steps to protect individuals' personal data and comply with the provisions of applicable regulations. 4. Openness: This principle emphasizes transparent access and processing of personal data, ensuring that individuals can access their personal data and understand how it is used. 5. Integrity: This principle emphasizes the need to protect personal data from unauthorized access, disclosure, or modification. Companies are expected to take steps to prevent the misuse of individuals' personal data. 6. Limitation of Data Use: This principle emphasizes that the use of personal data should be limited to agreed-upon purposes. Companies should not use personal data for other purposes without obtaining prior consent from the individuals involved[36].

d. Individual Rights: Active Protection

Both nations ensure the protection of individual rights related to their personal data. In Indonesia, there is a strong emphasis on the right to access, correct, and delete data, which is considered an integral aspect in safeguarding individual privacy[37]. Similarly, France, in alignment with Indonesia, not only underscores fundamental principles but also reinforces individual rights in the management of personal data. Beyond transparency and accountability, France emphasizes the right to protest (oppose) the use of data and ensures the ability to transfer data to other parties (portability) as a crucial pillar of individual human rights. Their shared commitment to these rights aims to guarantee fair and transparent data management, aligning with the privacy policies of each respective country.

e. Sanctions and Law Enforcement

Both jurisdictions establish sanctions and law enforcement mechanisms to safeguard personal data. In Indonesia, violations may result in administrative and criminal penalties[38].

[35] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi Pasal 5
[36] Article 5 GDPR Principles Relating To Processing Of Personal Data
[37] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi pasal 16
[38] Undang-Undang Nomor 27 tahun 2022 Pasal 42.

In accordance with the GDPR, France imposes significant sanctions, including fines that can reach a certain percentage of the company's annual turnover. Despite the existence of these sanctions, the implementation and level of legal enforcement may vary[39].

The Best Learning for Indonesia from Comparative Legal Studies with France

The most valuable lesson that Indonesia can draw from the comparative study of data protection laws between Indonesia and France is as follows:

a. Principles of Transparency and Integrity

France underscores the paramount importance of the principles of transparency and integrity in safeguarding personal data. Transparency signifies that personal data should be accessed and processed in a transparent manner, while integrity emphasizes safeguarding data from unauthorized access, disclosure, or modification. Indonesia may contemplate integrating these principles into its Personal Data Protection Law (PDPL). Examples of potential actions include urging companies to provide more transparent information to individuals regarding the use of their personal data, such as the purpose of data collection, the categories of data collected, and the third parties who will receive such data.

b. Right to Data Portability

France has granted individuals the right to transfer their personal data from one company to another, thereby enhancing individual control over their data. Indonesia may contemplate adopting a similar right within its Personal Data Protection Act (UU PDP). A illustrative measure could involve incorporating provisions into the UU PDP, affording individuals the right to transfer their personal data by requesting companies to provide the data in a readable and transferable format. This step would empower individuals and align Indonesia's data protection framework with international standards.

c. Data Protection Authority's Strength

The CNIL, the data protection authority in France, wields formidable power in enforcing the Personal Data Protection Act, including issuing warnings, imposing fines, or halting the activities of companies that violate the law. Similarly, the Indonesian Personal Data Protection Authority (OPDP) must also possess comparable authority to enforce the Personal Data Protection Act. A concrete measure to achieve this could involve granting additional powers to the OPDP, allowing it to conduct independent investigations without relying on individual reports. This would enable swift action against personal data breaches, ensuring a more proactive approach to enforcement.

By implementing these best practices, Indonesia stands poised to enhance the protection of personal data, strengthen individual rights, and ensure effective law enforcement in accordance with both national and international standards.

CONCLUSION

The safeguarding of personal data has become increasingly crucial in the digital era, where the escalating use of digital platforms can lead to data breaches if not handled responsibly. Both Indonesia and France have endeavored to establish frameworks governing the protection of personal data. In France, the General Data Protection Regulation (GDPR) serves as the European Union-level regulation providing comprehensive guidance on the management of personal data. The French Data Protection Act has been modified to align with GDPR provisions, and the National Commission on Informatics and Liberties (CNIL) is entrusted with enforcing data protection rules. Fundamentally, Indonesia and France share core principles of data protection, such as fairness, transparency, and accountability. However, there are nuanced emphases, with Indonesia underscoring fairness and accountability, while France highlights openness and integrity. Individual rights also take

[39] Article 83 - 84 GDPR Remedies, liability and penalties Principles relating to processing of personal data

center stage, as both countries affirm the rights to access, rectify, and erase data. In line with GDPR, France places particular emphasis on the rights to object and data portability, ensuring individuals have robust control over their personal data. Indonesia can draw valuable lessons from France in integrating principles of openness, the right to data portability, and empowering the data protection authority in the Personal Data Protection Act (PDPA). By implementing these insights, Indonesia can fortify personal data protection, ensure individual rights are safeguarded, and create a digital environment that is secure and trustworthy.

Based on the findings of this research, recommendations include: 1) Indonesia may consider incorporating the right to data portability into the PDPA. This right would enable individuals to transfer their personal data from one company to another, enhancing their control over personal information; 2) Strengthening the Personal Data Protection Authority (PDPA). The PDPA should be endowed with greater power and authority in enforcing the PDPA. This may involve granting the PDPA the authority to conduct independent investigations without waiting for reports from individuals, enabling swift action against personal data breaches; 3) Emphasis on education and public awareness. It is crucial to enhance public understanding of their rights regarding personal data and how to protect privacy. Educational campaigns and awareness initiatives can provide individuals with a better understanding of the importance of data protection and how to manage their consent regarding data usage.

REFERENCES

Afnesia, U., & Ayunda, R. (2021). Perlindungan Data Diri Peminjam Dalam Transaksi Pinjaman Online: Kajian Perspektif Perlindungan Konsumen Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(3), 1035-1044.

Amboro, F. Y. P., & Puspita, V. (2021, March). Perlindungan Hukum Atas Data Pribadi (Studi Perbandingan Hukum Indonesia dan Norwegia). In *CoMBInES-Conference on Management, Business, Innovation, Education and Social Sciences* (Vol. 1, No. 1, pp. 415-427).

Anjawai, N. B., Amboro, F. Y. P., & Hutauruk, R. H. (2022). Perbandingan Perlindungan Hukum Terkait Data Pribadi di Indonesia dan Jerman. *AL-MANHAJ: Jurnal Hukum dan Pranata Sosial Islam*, *4*(2), 207-218.

CNN Indonesia.com. 2022. "10 Kasus Kebocoran Data 2022: Bjorka Dominan, Ramai-Ramai Bantah", (https://www.cnnindonesia.com/teknologi/20221230125430-192-894094/10-kasus-kebocoran-data-2022-bjorka-dominan-ramai-ramai-bantah/2, diakses 1 Juni 2023).

Delpiero, M., Reynaldi, F. A., Ningdiah, I. U., & Muthmainnah, N. (2021). Analisis Yuridis Kebijakan Privasi dan Pertanggungjawaban Online Marketplace Dalam Perlindungan Data Pribadi Pengguna Pada Kasus Kebocoran Data. *Padjadjaran Law Review,* 9(1).

Disemadi, H. S. (2021). Urgensi regulasi khusus dan pemanfaatan artificial intelligence dalam mewujudkan perlindungan data pribadi di Indonesia. *Jurnal Wawasan Yuridika*, *5*(2), 177-199.

Disemadi, H. S. (2022). Lenses of Legal Research: A Descriptive Essay on Legal Research Methodologies. *Journal of Judicial Review*, *24*(2), 289-304.

Disemadi, H. S., & Budi, H. S. (2023). Enhancing Trade Secret Protection amidst E-commerce Advancements: Navigating the Cybersecurity Conundrum. *Jurnal Wawasan Yuridika*, *7*(1), 21-45.

Disemadi, H. S., & Prasetyo, D. (2021). Tanda Tangan Elektronik pada Transaksi Jual Beli Online: Suatu Kajian Hukum Keamanan Data Konsumen di Indonesia. *Wajah Hukum*, *5*(1), 13-20.

Disemadi, H. S., Sudirman, L., Girsang, J., & Aninda, A. M. (2023). Perlindungan Data Pribadi di Era Digital: Mengapa Kita Perlu Peduli?. *Sang Sewagati Journal*, *1*(2), 66-90.

Fikri, M., & Rusdiana, S. (2023). Ruang Lingkup Perlindungan Data Pribadi: Kajian Hukum Posistif Indonesia. *Ganesha Law Review,* 5(1), 39-57.

General Data Protection Regulation

Hartono, J., AW, A. M., Nugraha, X., & Felicia, S. A. (2023). Failing to Protect Personal Data: Key Aspects of Electronic System Operators' Agreements. *Barelang Journal of Legal Studies*, *1*(1), 31-55.

Mardiana, N., & Meilan, A. (2023). Urgensi Perlindungan Data Pribadi Dalam Prespektif Hak Asasi Manusia. *Jurnal Rechten: Riset Hukum Dan Hak Asasi Manusia,* 5(1), 16-23. H

Marzuki, M. (2017). *Penelitian Hukum: Edisi Revisi*. Prenada Media.

Purnama, T. D., & Alhakim, A. (2021). Pentingnya Uu Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia. *Jurnal Komunitas Yustisia*, *4*(3), 1056-1064.

Ramadhani, S. A. (2022). Komparasi Perlindungan Data Pribadi di Indonesia dan Uni Eropa. *Jurnal Hukum Lex Generalis*, *3*(1), 73-84.

Rizal, M. S. (2019). Perbandingan Perlindungan Data Pribadi Indonesia dan Malaysia. *Jurnal Cakrawala Hukum,* 10(2), 218-227.

Sautunnida, L. (2018). Urgensi Undang-Undang Perlindungan Data Pribadi di Indonesia: Studi Perbandingan Hukum Inggris dan Malaysia. *Kanun Jurnal Ilmu Hukum*, 20(2), 369-384.

Stevani, W., & Sudirman, L. (2021). Urgensi Perlindungan Data Pengguna Financial Technology terhadap Aksi Kejahatan Online di Indonesia. *Journal of Judicial Review*, *23*(2), 197-216.

Sudirman, L., Disemadi, H. S., & Aninda, A. M. (2023). Comparative Analysis of Personal Data Protection Laws in Indonesia and Thailand: A Legal Framework Perspective. *JED (Jurnal Etika Demokrasi)*, *8*(4), 497-510.

Sudirman, L., Situmeang, A., & Fiona, F. (2023). Enhancing Geographical Indications Product Protection: A Comparative Study of Indonesia and India. *Journal of Judicial Review*, *25*(2), 287-312.

Sylfia, A., Amrullah, M. F., & Djaja, H. (2021). Tanggungjawab Yuridis PT. Tokopedia atas Kebocoran Data Pribadi dan Privasi Konsumen Dalam Transaksi Online. *Bhirawa Law Journal*, 2(1), 21-27.

Tsamara, N. (2021). Perbandingan Aturan Perlindungan Privasi Atas Data Pribadi Antara Indonesia Dengan Beberapa Negara. *Jurnal Suara Hukum*, *3*(1), 53-84.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 Tentang Perlindungan Data Pribadi

Wibowo, M. H., & Fatimah, N. (2017). Ancaman phishing terhadap pengguna sosial media dalam dunia cyber crime. *JOEICT (Jurnal of Education and Information Communication Technology),* 1(1), 1-2.

Winarso, T., Disemadi, H. S., & Prananingtyas, P. (2020). Protection of private data consumers p2p lending as part of e-commerce business in indonesia. *Tadulako Law Review*, 5(2), 206-221.

Yuniarti, S. (2022). Petugas/Pejabat Pelindungan Data Pribadi dalam Ekosistem Perlindungan Data Pribadi: Indonesia, Uni Eropa dan Singapura. *Business Economic, Communication, and Social Sciences Journal (BECOSS),* 4(2), 111-120.