

Digital Platform Power Play: Indonesian and European Union Law Perspective

Hufron Hufron ^a, Sultoni Fikri ^a, Syofyan Hadi ^a, Ievgenii Shulga ^b,
Agung Satryo Wibowo ^a

^a Faculty of Law, Universitas 17 Agustus 1945 Surabaya, Indonesia

^b National University of Life and Environmental Sciences of Ukraine

✉ Corresponding email: hufron@untag-sby.ac.id

Abstract

Plenty aspect of human life across various regions, also Indonesia, utilizes electronic systems for a multitude of activities, and involving digital platforms. The concept of Digital Platform Powerplay is linked to the digital market and personal data protection. In Indonesia, the regulatory framework governing digital markets and personal data primarily relies on Law No. 11/2008 concerning Electronic Information and Transactions, which has undergone two amendments: Law No. 19/2016 amending Law No. 11/2008, and Law No. 1/2024 amending Law No. 11/2008 for the second time and Law No. 27/2022 concerning Personal Data Protection. As a implementation regulation Government Regulation No. 80/2019 concerning Electronic Commerce and Government Regulation No. 71/2019 concerning the Implementation of Electronic Systems and Transactions further elaborate on these regulations. These legal provisions are intended to provide legal certainty for users. It is

essential to review all regulations related to electronic systems and digital platforms by comparing them with the regulatory frameworks in the European Union. The study addresses two primary issues: 1) the legal regulation of digital markets from the perspective of Indonesian positive law, and 2) the legal regulation of digital markets from the perspective of European Union law. This research employs normative legal research methodologies, utilizing both statutory and comparative approaches. The findings of this study suggest that Indonesia should consider adopting the European Union's Digital Markets Act and Personal Data Protection regulations by amending Law No. 11/2008 concerning Electronic Information and Transactions and its amendments, with particular emphasis on aspects related to Digital Platform Powerplay.

KEYWORDS *Digital Platform Powerplay, Digital Market, Personal Data*

Introduction

The rapid advancement of information technology in the current era has led to its integration into nearly every facet of human life. Technology and Information Systems have become indispensable elements across various domains. A major driver of this technological progress is globalization, which has increasingly penetrated societal structures, particularly in Indonesia. Globalization can be understood as a social, historical, and natural process that facilitates the interconnection of nations worldwide, leading to the emergence of new global frameworks and the unification of systems by dissolving geographical, economic, and cultural boundaries among global communities. This technological progression has resulted in profound transformations in multiple spheres of human existence. Although digital or cyber activities occur within a virtual space, these actions nonetheless constitute real and legally recognized conduct, signifying the tangible implications of such technological advancements within legal frameworks.¹

According to data from the Indonesian Internet Service Providers Association (APJII), as of 2024, the number of internet users in Indonesia has reached 221,563,479 individuals.² This signifies that more than half of the Indonesian population now relies on internet access for daily activities. APJII

¹ Asih Handayanti, "The Role of Cyber Law in The Use of Technology in Mass Media," *Legal Brief* 11, no. 5 (2022): 2722–4643, <https://doi.org/10.35335/legal.the>.

² APJII, "Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang," Asosiasi Penyelenggara Jasa Internet Indonesia, 2023, <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>.

further indicates that internet usage in Indonesia has experienced substantial growth over the past five years, beginning in 2018. Notably, Generation Z constitutes the largest demographic in the digital sphere, comprising 34.40% of total users. The increasing prevalence of internet use, particularly among younger generations, necessitates a comprehensive legal response to address the challenges arising from this digital transformation. Issues related to privacy, data protection, and cyber regulations are of critical importance as the digital economy continues to expand. This demographic shift underscores the urgency for the development of robust legal frameworks that can accommodate the complexities of digital interaction, ensuring both the protection of individual rights and the regulation of online activities in accordance with legal standards.

As in the context of social life, relationships between two or more individuals also occur within the realm of technology and information systems, including in social media, electronic transactions, and other forms of electronic information. Therefore, it is essential to have a regulatory framework that governs interactions within the scope of technology. Law No. 11 of 2008 on Electronic Information and Transactions, which has undergone two amendments—namely Law No. 19 of 2016 amending Law No. 11 of 2008, and Law No. 1 of 2024 constituting the second amendment—serves as the fundamental legal norm governing societal life in relation to technology and information systems. The establishment of such a legal framework is crucial for protecting all citizens as they navigate the internet, given that information systems and electronic platforms often involve the handling of personal data belonging to individual users. These regulations are designed to protect and safeguard the flow of cyber traffic from various forms of crime and violations within the technological sphere, ensuring that legal norms effectively regulate the increasingly complex and interconnected digital landscape.

The Indonesian government, in its ongoing efforts to enhance the protection of every citizen's rights, particularly the right to feel secure in conducting societal activities, has consistently sought to develop regulations that are responsive to the dynamic changes in society. In addition to Law No. 1/2024 concerning Electronic Information and Transactions and also the country has enacted Law No. 27 of 2022 concerning Personal Data Protection (Law No. 27/2022). Indonesia has also established other pertinent regulations, such as Ministry of Communication and Informatics Regulation No. 5 of 2020 on Private Scope Electronic Systems Operators, which was amended by Ministry of Communication and Informatics Regulation No. 10 of 2021. Furthermore, Presidential Regulation No. 32 of 2024 on the Responsibility of Digital Platform Companies to Support Quality Journalism (Perpres No.

32/2024). These legal instruments reflect the government's commitment to aligning regulatory frameworks with evolving technological advancements and societal needs. They play a critical role in safeguarding individual rights within the increasingly complex digital ecosystem, addressing issues such as data privacy, electronic system governance, and corporate responsibility in the digital age.

Jeane Neltje, in her scholarly work titled, "Analisis Perlindungan Data Pribadi Terkait UU No. 27 Tahun 2022" observes that the development of personal data protection in Indonesia has seen notable progress. Nevertheless, several obstacles persist, particularly with regard to Law No. 27/2022. These challenges include insufficient regulatory oversight and enforcement mechanisms, as well as the rapid evolution of technology, which increases the susceptibility of personal data to breaches.³ Kadek Rima, in her journal article, "Menjaga Privasi di Era Digital: Perlindungan Data Pribadi di Indonesia" offers a comparative analysis of Indonesia's personal data protection framework with those of other jurisdictions, including Singapore, Malaysia, Hong Kong, and South Korea. Rima underscores the necessity for the Indonesian government to ensure that all business and governmental entities, such as hospitals, public service applications, the banking sector, and other industries, adhere to the provisions of Law No. 27/2022. These scholarly analyses underscore the critical need for more robust regulatory frameworks and enforcement strategies to keep pace with the rapid technological advancements that exacerbate vulnerabilities in personal data protection. Moreover, they highlight the importance of aligning Indonesia's legal frameworks with international best practices, ensuring that personal data is adequately safeguarded in an increasingly interconnected digital environment.⁴

³ Jeane Neltje Saly et al., "Analisis Perlindungan Data Pribadi Terkait UU No.27 Tahun 2022," *Jurnal Serina Sosial Humaniora* 1, no. 3 (2023): 145–153, <https://doi.org/10.24912/jssh.v1i3.28615153>.

⁴ Kadek Rima Anggen Suari and I Made Sarjana, "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia," *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–146, <https://doi.org/10.38043/jah.v6i1.4484>. Kadek also mentioned that the PDP Law adopts some general principles found in the European Union's General Data Protection Regulation (GDPR). The GDPR provides a robust framework for protecting the personal data of EU citizens and regulates how data may be collected, processed and stored. Judging from what was written, it is said that it is still possible to hack personal data even though the PDP Law has been born. So that the government is expected to provide protection for the personal data of certain individuals or groups such as data on children and other vulnerable groups.

The concept of Digital Platform PowerPlay primarily denotes the intense competitive dynamics among major corporations that either leverage or directly operate digital platforms. These dominant entities, including giants such as Google, Facebook, Instagram, TikTok, and others, significantly influence the contemporary technological media landscape. This research is designed to analyze and compare the regulatory frameworks related to technology and information systems in Indonesia and the European Union. Consequently, the study will address the following research questions: How is digital/cyber law regulated under the framework of Indonesian positive law? And how is digital/cyber law regulated under the framework of European Union law?

The objective of this research is to provide a comparative analysis of the legal regulations governing digital and cyber activities in Indonesia and the European Union. By examining the legal approaches and regulatory mechanisms in these jurisdictions, the study aims to elucidate the similarities and differences between their frameworks. This comparative analysis will contribute to a more nuanced understanding of how different legal systems address the challenges posed by digital platforms and may offer insights for the development of more effective regulatory strategies in the digital era.

This research employs a normative legal research methodology. It utilizes statutory, conceptual, and comparative approaches. The study involves the collection of legal materials through library research and employs a descriptive analysis technique, complemented by prescriptive analysis.

Legal Framework for Digital & Cyber Regulations in Indonesia

A. Cyberlaw & Personal Data Protection: A Legal Perspective

The protection of personal data within the context of human rights is fundamentally integral to the concepts of individual dignity and freedom.⁵ The right to privacy, as enshrined in various human rights conventions, transcends the mere ability to conceal or control information. It represents a fundamental

⁵ Rosihan Luthfi, "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia," *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36, <https://doi.org/10.59188/jurnalsostech.v2i5.336>.

recognition of the intrinsic value of human beings.⁶ Privacy provides a critical space for individuals to live autonomously, shielded from external intrusions that might compromise their personal existence and integrity.⁷ Personal data encompasses more than just technical digital or physical information; it includes the most intimate aspects of an individual's life. Such data reflects personal choices, preferences, and social connections that collectively shape one's identity. Consequently, unauthorized exposure or exploitation of this data signifies a profound human rights violation. This breach undermines an individual's right to govern how they are perceived and utilized within social and political spheres. It embodies the principle that individuals should not be reduced to mere objects subject to surveillance, control, or exploitation by more powerful entities, whether governmental or private.

The protection of personal data must, therefore, be conceptualized as a shared moral obligation that transcends the mere provision of legal frameworks.⁸ In the contemporary landscape, where personal data is extensively recorded and stored online across both public and private sectors, and with the advent of increasingly sophisticated technological capabilities, the accessibility of such data is markedly enhanced. This accessibility heightens the risk of cybercrimes that inflict harm, such as unauthorized dissemination of personal information or its misuse for various ulterior purposes. The implications of such breaches extend beyond the immediate harm inflicted upon individuals whose personal data has been compromised. They also encompass significant repercussions for entities managing electronic media platforms, which may experience reputational damage and a subsequent decline in user trust and engagement due to the mishandling or exposure of personal data. Thus, safeguarding personal data necessitates a comprehensive approach that integrates legal, ethical, and technological considerations to effectively mitigate

⁶ Upik Mutiara and Romi Maulana, "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi," *Indonesian Journal of Law and Policy Studies* 1, no. 1 (2020): 42, <https://doi.org/10.31000/ijlp.v1i1.2648>.

⁷ Michael Huggins, "The Right to Privacy: An Argument for A Non-Derivative Right to Privacy," *New York State Bar Association (NYSBA)* (New York University, 2011), <https://doi.org/10.2139/ssrn.2416653>.

⁸ Maria Tzanou, "Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right," *International Data Privacy Law* 3, no. 2 (May 1, 2013): 88–99, <https://doi.org/10.1093/idpl/ipt004>. See also Maja Brkan, "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning," *German Law Journal* 20, no. 6 (2019): 864–83, <https://doi.org/10.1017/glj.2019.66>.

risks and uphold individual privacy rights in an increasingly interconnected digital environment.⁹

Personal data represents a critical element of confidentiality that must be rigorously protected by electronic media operators.¹⁰ The state is tasked with ensuring the establishment of a legal framework that not only guards against the misuse of such data but also reinforces broader human rights, including the right to an inviolable personal space free from external intrusion. The objective of this protection is to secure the individual rights of citizens concerning personal security, to affirm the importance of personal data protection, and to enhance public awareness regarding these issues. Infringements upon personal data are inherently linked to violations of human dignity, as each instance of data misuse involves an unwarranted intrusion into an individual's personal narrative. Thus, safeguarding personal data is fundamentally connected to upholding the intrinsic value of individuals and ensuring their right to privacy is both recognized and protected.¹¹ This underscores the necessity for a comprehensive approach to data protection that integrates legal, ethical, and societal considerations.

Moreover, the protection of personal data functions as a critical instrument in bolstering other human rights enshrined within international human rights frameworks, including freedoms of expression, assembly, and association. In an era characterized by advanced surveillance technologies, personal data often becomes a tool for social control. Absent robust protection mechanisms, there exists a significant risk of gradual erosion of these fundamental freedoms. Consequently, the safeguarding of personal data is not merely an ancillary issue but a fundamental aspect of a holistic approach to human rights protection. It underscores the principle that individuals have an intrinsic right to full control over the most intimate aspects of their personal lives. Enhancing public awareness regarding the human rights implications of data protection transcends the realm of digital security and delves into the broader context of respecting human dignity in a rapidly interconnected

⁹ Thiara Dewi Purnama and Abdurrahman Alhakim, "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia," *E-Journal Komunitas Yustisia* 4, no. 3 (2021): 273–83.

¹⁰ Kornelius Benuf, Siti Mahmudah, and Ery Agus Priyono, "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia," *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (2019): 145–60, <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>.

¹¹ Danrivanto Budhijanto, *Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity* (Bandung: PT Refika Aditama, 2023).

world.¹² This protection acts as a defense against dehumanization, where individuals may be reduced to mere data points subject to exploitation. Conversely, each advancement in privacy protection represents a commitment to the recognition and preservation of the intrinsic value and irreplaceability of the human person.

At its core, the protection of personal data represents a profound reflection of the moral and ethical obligations to preserve individual dignity and autonomy in the digital era. Lex Informatica, as a normative construct arising from technology-mediated communication and interaction systems, transcends the mere technicalities of legal regulation. It serves as a manifestation of the universal values that underpin human rights, with a particular focus on the rights to privacy and control over personal information. Lex Informatica emerges as a critical response to the social transformation that has fundamentally altered the ways in which individuals communicate and interact in cyberspace. In this context, personal information and data have become commodities that are susceptible to unchecked exploitation if not adequately regulated. Thus, Lex Informatica must be recognized as a fundamental necessity by policymakers—not merely as a regulatory mechanism but as a foundational framework that safeguards individual rights against unauthorized control and surveillance.¹³ This normative framework functions as both an ethical and moral guide, underscoring that behind every piece of data is an individual with inherent rights to personal autonomy. The failure to acknowledge the significance of Lex Informatica equates to reducing human beings to mere objects subject to technological control, thereby neglecting the essential respect for individual freedoms and dignity.

Regulation concerning personal data protection, as stipulated by Article 28G, Paragraph (1) of the 1945 Constitution of the Republic of Indonesia (UUD NRI 1945), represents a fundamental reflection of privacy rights, which are integral to human dignity. This right encompasses not only physical protection but also extends to the digital realm, acknowledging the pervasive

¹² Valentin M. Pfisterer, “The Right to Privacy—a Fundamental Right in Search of Its Identity: Uncovering the CJEU’s Flawed Concept of the Right to Privacy,” *German Law Journal* 20, no. 5 (2019): 722–33, <https://doi.org/10.1017/glj.2019.57>.

¹³ Christos Dimitrou, “Lex Informatica and Legal Regime: Their Relationship,” *Electronic Journal*, 2015, <https://doi.org/10.2139/SSRN.2626941>. See also Fahmi Ali Ramdhani, et.al. “Lex Informatica Theory Approach as An Architecture To Prevent And Handle Hate Speech In Cyberspace,” *Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/Journal of Tianjin University Science and Technology* 56, no. 10 (2023): 231–42, <https://doi.org/10.5281/zenodo.8424414>.

role of technology and digital communication in contemporary social interactions. In the modern context, personal data—encompassing identity, preferences, and personal information—serves as a crucial extension of individual autonomy, necessitating stringent safeguards against unauthorized access and misuse. Lex Informatica, emerging from the evolving landscape of information technology, seeks to address deficiencies in the existing legal framework pertaining to data management within the digital environment. This normative framework underscores that legal structures must evolve in tandem with advancements in social and economic interactions driven by the collection, storage, and distribution of personal data. It provides a philosophical foundation that positions privacy rights not as isolated entitlements but as central to the protection of human dignity in a technology-driven context. The enactment of Law No. 27 of 2022 reflects a legislative response to increasing concerns over personal data misuse, which poses significant threats to privacy rights in Indonesia. Misuse of personal data results in a loss of control over one's information and exposes individuals to risks of dignity infringement and security breaches. This situation is in direct conflict with the essence of human rights as articulated in Article 28G, Paragraph (1) of the UUD NRI 1945, which underscores the importance of safeguarding personal security and autonomy from undue threats or coercion. Thus, the regulation serves to fortify the protection of personal data as an essential component of broader human rights protections in an increasingly interconnected and digitalized world.

In the domain of policy formulation for information management and regulatory development within society, Lex Informatica exhibits several distinctive characteristics: 1. Lex Informatica operates beyond national territorial constraints, as a framework for technological regulation, Lex Informatica is not confined by geographical boundaries. It addresses challenges and issues that inherently cross national borders, reflecting the inherently global nature of digital interactions and data management; 2. Lex Informatica supports regulatory customization through diverse technical mechanisms, the framework allows for the adaptation and customization of regulations to accommodate a wide array of technical mechanisms and requirements. This adaptability is essential for addressing the specific needs and technological contexts of various digital environments; 3. Lex Informatica leverages mechanisms of self-regulation and internal compliance monitoring. The regulatory framework benefits from integrated self-regulation and internal monitoring systems designed to ensure adherence to established standards. This approach enhances the efficacy of compliance efforts and fosters proactive governance in technological and informational practices.

The legal framework for personal data protection is conceptually rooted in the *Sui Generis Lex Habeas Data*. Law No. 27/2022, which embodies *Lex Habeas Data*, delineates several foundational legislative principles: 1. Principle of Protection. The processing of personal data must be conducted with stringent measures to safeguard the data from misuse. This principle underscores the necessity for protective mechanisms to prevent unauthorized or inappropriate use of personal data; 2. Principle of Legal Certainty. All personal data processing activities must be grounded in legal authority to ensure effective protection and facilitate lawful recognition and enforcement both within judicial contexts and beyond. This principle aims to provide a clear legal framework for data handling, ensuring that actions are consistent with established legal standards; 3. Principle of Public Interest. The enforcement of personal data protection must consider whether such measures align with broader public interests. This encompasses the needs of state administration, as well as national defense and security concerns. The principle highlights the balance between individual rights and collective societal needs; 4. Principle of Utility. Regulations pertaining to personal data protection must be designed to benefit national interests, particularly in the pursuit of general welfare. This principle emphasizes the importance of aligning data protection laws with the overarching goals of societal well-being; 5. Principle of Caution. All entities involved in the processing and oversight of personal data must exercise meticulous care to prevent any potential harm. This principle advocates for a prudent approach to data handling to mitigate risks and protect individuals from adverse consequences; 6. Principle of Balance. Effective personal data protection requires balancing the individual's right to privacy with the legitimate interests of the state, based on public needs. This principle seeks to harmonize individual privacy rights with the necessary interests of governmental and societal functions; 7. Principle of Accountability. Entities responsible for the oversight and processing of personal data must operate with a high degree of accountability. This principle ensures that all parties involved in data handling adhere to their obligations and maintain a balance between rights and responsibilities; 8. Principle of Confidentiality. Personal data must be treated as confidential and cannot be disclosed without appropriate consent. This principle underscores the necessity of protecting personal data from unauthorized access and ensuring that data processing activities are conducted in accordance with established confidentiality norms.

As a legal framework emerging from the complexities of the digital era, Cyberlaw introduces a novel dimension to the understanding of regulations interacting with technology. This legal domain arises as a response to the

fundamental shifts involving individual rights and public interests within the virtual realm.¹⁴ Within this paradigm, Cyberlaw implicitly redefines traditional legal concepts such as Copyright, Trademark, and Defamation, which are now evolving within an increasingly abstract and expansive digital landscape. Cyberlaw extends beyond merely addressing existing legal dimensions; it introduces a normative structure that probes deeper into the concept of Privacy—recognized as a fundamental human right that requires safeguarding but is frequently threatened in the digital context. The protection of privacy, in this instance, becomes critically important as technology blurs the distinction between private life and public domain. The concept of Duty of Care, traditionally emphasized in civil liability contexts, acquires a new interpretation in the digital age. Responsibilities now encompass not only physical actions but also the measures necessary to protect data and information integral to digital human interaction. Cyberlaw functions as a conduit between the physical and virtual realms, presenting new methodologies for legal problem-solving and offering ethical guidance in a continually evolving digital ecosystem. By addressing a spectrum of issues from intellectual property rights to privacy and defamation, Cyberlaw demonstrates how the legal system endeavors to keep pace with and potentially steer technological advancement. Cyberlaw represents an effort to adapt legal principles to the intangible and often unpredictable digital world, underscoring the necessity for responsibility and caution in the utilization of technology that increasingly permeates all aspects of human life.

Law No. 27/2022, as one of the most recent regulations for the protection of personal data, provides the following legal framework:

1. Legal Subjects of Personal Data under Articles 1 *jo.* 5-10 of Law No. 27/2022

Law No. 27/2022 defines "*legal subjects of personal data*" as individuals whose personal data can be identified either independently or in conjunction with other information, through electronic or non-electronic means. This distinction is crucial in differentiating between "*legal subjects of personal data*" and "*data subjects*." In this context, a "data subject" refers to an individual to whom personal data relates. Data subjects possess a suite of inherent rights

¹⁴ Nigel Miller, "Cyberlaw — Legal Issues Online," *Computer Audit Update*, no. 12 (1995): 4–9, [https://doi.org/10.1016/S0960-2593\(00\)80061-0](https://doi.org/10.1016/S0960-2593(00)80061-0). See also Cius Borges et al., "Perspectivas para o ensino de ciberdireito a partir das novas diretrizes curriculares para os cursos de direito no Brasil: Perspectives for the study of cyber law from the new curricular guidelines for law courses in Brazil," *Revista Jurídica* 01, no. 54 (2019): 639–60, <https://doi.org/10.6084/m9.figshare.12093861>.

under this law, including the right to be informed about the clarity of their identity, the legal grounds for processing their data, the purpose of data requests and usage, and the accountability of the entities requesting the data.

Data subjects are entitled to rectify, update, and/or amend inaccuracies in their personal data in accordance with the purposes of data processing. Moreover, data subjects have the right to access and obtain copies of their personal data, to cease processing, and to delete or destroy their personal data. They also retain the right to withdraw previously granted consent for data processing by data controllers and to challenge decisions based solely on automated processing, including profiling that results in legal consequences or impacts on the data subject. Law No. 27/2022 serves as a significant framework for the protection of human rights, ensuring that the rights of individuals or data subjects are safeguarded to prevent any potential harm. This legislative approach underscores the fundamental principle that personal data protection is integral to upholding human dignity and autonomy in an increasingly data-driven world.

2. Nature of Personal Data under Article 4 of Law No. 27/2022

Law No. 27/2022 delineates the nature of personal data into two primary categories: specific and general. This bifurcation is essential for the tailored application of protective measures and regulatory frameworks. This category encompasses data that, due to its sensitive nature, requires heightened safeguards to prevent misuse and protect individual privacy. Specific personal data includes: Health data and information; Biometric data; Genetic data; Criminal records; Data pertaining to minors; Personal financial data; Any other data as defined by relevant regulations. General Personal Data, this category includes less sensitive data that still identifies individuals but does not entail the same level of risk if disclosed.

General personal data comprises: Full name; Gender; Citizenship; Religion; Marital status; Any other personal data combined to identify an individual. This classification framework is pivotal in ensuring that personal data is handled with the appropriate level of protection, aligning with the principles of data privacy and regulatory compliance. It underscores the necessity of differentiated treatment based on the sensitivity and potential impact of data disclosure on individuals' privacy and security.

3. Data Controllers under Article 1 *jo*. Article 19 of Law No. 27/2022

Under Law No. 27/2022, the term "*data controller*" encompasses any individual, public authority, or international organization that independently

or jointly determines the purposes and means of processing personal data. The concept of the data controller is pivotal within the framework of data protection law as it designates the entity responsible for the governance of personal data processing activities. This responsibility includes the establishment and implementation of policies and procedures that ensure compliance with legal standards, safeguarding the rights of data subjects, and maintaining data security.

Data controllers are tasked with defining the objectives for data processing, establishing the methods for achieving these objectives, and overseeing the execution of processing activities. They are also accountable for ensuring that data processing adheres to the principles of legality, fairness, and transparency, as well as for addressing any potential breaches or unauthorized access to personal data.

4. Prohibitions on the Use of Personal Data under Articles 65-66 of Law No. 27/2022

Law No. 27/2022 establishes several prohibitions regarding the use of personal data. Specifically, it is unlawful for any individual to:

- a. Acquire or collect personal data that does not belong to them for the purpose of benefiting themselves or others, which may result in harm to the data subject;
- b. Disclose personal data that does not belong to them;
- c. Utilize personal data that does not belong to them;
- d. Create false personal data or falsify personal data with the intent to benefit themselves or others, potentially causing harm to others.

5. Sanctions for against of Personal Data Protection Law under Articles 57 *jo.* 67 of Law No. 27/2022

Law No. 27/2022 prescribes a dual framework of sanctions for violations related to personal data protection: administrative sanctions and criminal sanctions. Administrative sanctions under Law No. 27/2022 include: Issuance of a written warning; Suspension of personal data processing activities; Erasure or destruction of personal data; and Administrative fines. Administrative fines may be imposed by relevant authorities and can be as high as 2% of the annual revenue or annual receipts associated with the violation. Criminal sanctions encompass imprisonment and/or fines. Specific sanctions for violations include: For violations of Article 65(1) of Law No. 27/2022, imprisonment for up to 5 years and/or a fine not exceeding IDR 5,000,000,000 (five billion rupiah); For violations of Article 65(2) of Law No. 27/2022, imprisonment for up to 4 years

and/or a fine not exceeding IDR 4,000,000,000 (four billion rupiah); For violations of Article 66(3) of Law No. 27/2022, imprisonment for up to 5 years and/or a fine not exceeding IDR 5,000,000,000 (five billion rupiah); For violations of Article 66 of Law No. 27/2022, imprisonment for up to 6 years and/or a fine not exceeding IDR 6,000,000,000 (six billion rupiah). These sanctions aim to ensure compliance with personal data protection regulations and to deter unlawful activities that compromise the security and privacy of personal data.

From a utilitarian perspective, a thorough examination of the interplay between law, happiness, and societal welfare is essential.¹⁵ Utilitarianism contends that the law should be designed to maximize the greatest good for the greatest number, mitigate suffering, and promote social justice. Law No. 27/2022 reflects an attempt to harmonize the protection of individual rights to personal data with public interests in the lawful use of data. This aligns with utilitarian principles, which view law as a mechanism for advancing social welfare through effective regulation.

The provisions concerning legal subjects of personal data, as articulated in Articles 1 in conjunction with Articles 5 through 10, are aimed at protecting individuals in relation to their personal data. Within a utilitarian framework, this is significant as it addresses the potential misuse of data that could inflict harm on individuals. Such protections are crucial in maintaining a balance between personal and public interests, ensuring that the rights of data subjects to manage information about themselves are upheld. The legal rights to receive information about data usage, to correct or update erroneous data, and to delete personal data are integral components of this legislative framework. From a utilitarian standpoint, these rights serve to prevent potential harm and suffering. Thus, Law No. 27/2022 is functionally aligned with utilitarian principles by seeking to prevent suffering and enhance overall well-being, thereby ensuring that legal protections support both individual rights and broader social interests.

Furthermore, the regulation delineating personal data into specific and general categories, as outlined in Article 4, is consistent with the utilitarian perspective that advocates for the utmost protection of the most vulnerable aspects of individual life. Specific data, such as health information, biometric data, and personal financial details—given their significant potential to cause harm if improperly accessed or misused—are afforded heightened protection

¹⁵ Dhifa Nadhira Syadzwina, Dominikus Rato, and Bayu Dwi Anggono. “The Legal Position of Limited Partnership in Indonesia through the Perspective of the Philosophy of Utilitarianism,” *International Journal of Social Science and Education Research Studies* 03, no. 11 (2023): 2247–57, <https://doi.org/10.55677/ijssers/v03i11y2023-11>.

under this regulatory framework. This approach reflects an intention to not only mitigate direct individual harm but also to avert broader societal suffering by implementing a regulatory regime sensitive to the intrinsic value and risk associated with such data. Conversely, general data, which is more commonly employed for public administrative functions, remains protected but is subject to broader utilitarian considerations. This regulatory approach enables its use while balancing the maximization of public utility against the need to minimize individual risk. The principle of utilitarianism is thus embodied in this categorization, where the law strives to enhance overall social welfare and utility, while carefully managing the potential for individual harm. This alignment illustrates a commitment to utilitarian values, emphasizing both the enhancement of societal benefits and the reduction of potential suffering through judicious regulation of personal data.

As articulated in Article 1 in conjunction with Article 19 of the Law No. 27/2022, this statute institutionalizes mechanisms for ensuring accountability among data controllers, encompassing both individuals and public entities. The role of data controllers is pivotal in ensuring that data processing is conducted in a manner that aligns with the public interest while upholding the primacy of data subject protection. From a utilitarian perspective, this legal framework seeks to harmonize individual liberties with public safety, with the overarching goal of maximizing collective welfare.

The principle of accountability imposed on data controllers functions as a preventive measure designed to avert misuse, thereby reducing potential harm and enhancing overall social well-being. This approach resonates with utilitarian principles by minimizing suffering and promoting the greatest good for the greatest number. Additionally, the statutory prohibitions against the unlawful use of personal data, as delineated in Articles 65-66, underscore the law's commitment to safeguarding against the potential misuse and exploitation of personal data. The unauthorized appropriation of personal data for individual gain not only inflicts harm upon data subjects but also engenders systemic injustices, which, within a utilitarian framework, must be addressed to prevent societal suffering. These legal restrictions serve to mitigate undesirable risks while facilitating the legitimate use of data for broader public benefit. Thus, the regulation enshrined in this law ensures that a delicate balance between public advantage and individual rights protection is maintained, aligning with the fundamental tenets of utilitarian theory. This balance is essential for fostering a legal environment that both respects individual autonomy and advances the common good.

The sanctions articulated in Articles 57 and 67 of Law No. 27/2022, encompassing both administrative and criminal penalties, epitomize a judicial stance that emphasizes the prevention of violations that could lead to significant harm. In the context of utilitarian theory, sanctions are not solely punitive but are designed as preventative mechanisms to avert further detrimental consequences. Administrative sanctions, including written warnings, temporary suspension of data processing activities, and the imposition of fines, serve to ensure compliance and promote accountability among data controllers. The imposition of substantial fines, with a maximum of 2% of annual revenue, reflects a utilitarian approach aimed at discouraging non-compliance by creating a substantial deterrent. Similarly, criminal sanctions, which can involve imprisonment or significant fines, are intended to address more severe breaches and further reinforce the legal framework's capacity to deter misuse. From a utilitarian perspective, the rationale behind these sanctions is to mitigate the potential suffering and harm that could arise from improper handling of personal data. By establishing stringent penalties, the law seeks to prevent violations and ensure that individuals and entities involved in data processing are compelled to adhere to regulatory standards.

This approach aligns with the utilitarian principle of maximizing overall societal welfare by reducing harm and enhancing the effectiveness of data protection measures. The regulatory framework not only aims to penalize but also to proactively prevent potential abuses, thereby contributing to the broader objective of safeguarding individual rights and promoting societal well-being. The comprehensive nature of these sanctions demonstrates a commitment to upholding justice and ensuring that personal data protection remains robust and effective.

Thus, Law No. 27 of 2022, when examined through the framework of utilitarianism, is designed to strike an optimal equilibrium between safeguarding individual rights and addressing societal needs for data access. This legislation is crafted not merely to mitigate potential individual suffering but also to enhance public welfare through a framework of accountable and systematic regulation. In alignment with utilitarian principles, the law endeavors to maximize overall societal benefit by advancing data security for all stakeholders while concurrently minimizing the risks of harm that may result from data misuse. This approach reflects a commitment to achieving the greatest aggregate happiness by ensuring robust protection against potential abuses, thereby balancing the imperatives of individual privacy with the broader demands for data accessibility.

B. Regulation of Digital Economy & Electronic Transactions: A Legal Analysis

The rapid advancement of Information Technology has engendered profound transformations across all aspects of human life, particularly within the realm of transactional activities. This evolution introduces both beneficial and detrimental effects on human conduct. The digital economy and electronic transactions emerge as products of technological and informational progress. The underlying infrastructure and telecommunications systems are crucial for facilitating the exchange of information and electronic transactions among individuals. Initially conceptualized by Don Tapscott, The Digital Economy is characterized as a socio-economic system that functions as an intelligence space, incorporating information, various access mechanisms, capacities, and information processing. The components of The Digital Economy that can be distinctly identified include the technology, information, and communication (TIC) industries, e-commerce activities, and the digital distribution of goods and services.¹⁶ Atkinson defines the digital economy as an era where activities are predominantly represented by the use of information technology (IT)—encompassing hardware, software, applications, and telecommunications—in various economic contexts, including internal organizational operations. Thus, according to this definition, the digital economy constitutes an economic system predicated on electronic goods and services produced by electronic enterprises and transacted through electronic commerce.¹⁷

In 2019, Indonesia enacted Government Regulation No. 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP No. 71/2019), which superseded the earlier Government Regulation No. 82 of 2012 on the same subject (PP No. 82/2012). This legislative transition was driven by the recognition that PP No. 82/2012 no longer adequately addressed the evolving legal and technological requirements of contemporary society. PP No. 71/2019 provides a revised definition of Electronic Transactions as legal acts executed through the use of computers, computer networks, and/or other electronic media. This regulation underscores the importance of integrating personal data protection within the framework of digital economy transactions. According to PP No. 71/2019, Electronic System Providers are designated as

¹⁶ Don Tapscott, *The Digital Economy: Promise and Peril in the Age of Networked Intelligence* (New York: McGraw-Hill, 1995). pp. 2-4.

¹⁷ Ananthia Ayu D, Anindyajati Titis, and Abdul Ghoffar, *Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital* (Jakarta: Pusat Penelitian dan Pengkajian Perkara Mahkamah Konstitusi, 2019).

legal entities. An Electronic System Provider encompasses any individual, governmental body, business entity, or community that provides, manages, and/or operates Electronic Systems, either independently or in collaboration with others, for the purposes of serving Electronic System Users and/or third parties. As stipulated by PP No. 71/2019, Electronic System Providers are legally mandated to ensure that their systems do not host electronic information and/or documents that are prohibited under existing legislation. This regulatory framework is designed to safeguard the integrity and legality of electronic transactions while addressing the needs for robust data protection and compliance with legal standards.

Government Regulation No. 71 of 2019, which replaced Government Regulation No. 82 of 2012, establishes a framework for administrative sanctions in the realm of electronic systems and transactions. The sanctions delineated under this regulation encompass written warnings, administrative fines, temporary suspension of operations, termination of access, and/or removal from the registry. These administrative penalties are largely congruent with those outlined in Law No. 27 of 2022, reflecting a consistent approach to regulatory enforcement. In addition to administrative sanctions, the legal framework for addressing criminal violations related to electronic transactions is further elaborated in Law No. 11 of 2008 on Electronic Information and Transactions, which was amended by Law No. 19 of 2016, and subsequently by Law No. 1 of 2024. These statutes collectively provide a comprehensive legal basis for both administrative and criminal sanctions, ensuring robust oversight and accountability in the management and operation of electronic systems.

Electronic transactions inherently involve the use of electronic contracts or agreements. Law No. 1 of 2024, as a *Lex Generalis Digitalis*, establishes a foundational legislative framework for electronic contracts. Article 1, number 17, defines an electronic contract as an agreement formed between parties through an electronic system. These electronic contracts formalize the binding nature of electronic transactions between the parties involved. The detailed regulation of electronic contracts is further elaborated in Government Regulation No. 71 of 2019, which provides for the recognition of electronic contracts within the jurisdiction of Indonesia's virtual environment. According to Article 46 of Government Regulation No. 71 of 2019, electronic transactions can be based on electronic contracts or other contractual forms as agreed upon by the parties. This regulation also sets forth the criteria for the validity of electronic contracts, which are deemed valid if they meet several conditions: there must be mutual agreement between the parties; the contract must be executed by legally competent individuals or authorized representatives in

accordance with statutory requirements; it must encompass specific terms; and the subject matter of the transaction must not violate legal regulations, public morality, or public order. Furthermore, electronic contracts are also addressed in related regulations, specifically in Government Regulation No. 80 of 2019 concerning Electronic Commerce. This regulation is designed to govern electronic business activities to ensure a fair, transparent trading system and to safeguard national interests.¹⁸ Article 50 of Law No. 1 of 2024 provides that electronic commerce may employ electronic contracts or other contractual mechanisms to reflect the parties' agreements. However, under Article 57 of Law No. 1 of 2024, an electronic contract is considered automatically void if technical errors arise due to an electronic system being insecure, unreliable, or irresponsible. This provision underscores the necessity for secure and dependable electronic systems in maintaining the validity and enforceability of electronic contracts.

According to Richard Posner's economic analysis of law theory, digital economic regulation and electronic transactions should be assessed through the lens of how such regulations can enhance market efficiency, reduce transaction costs, and provide legal clarity and certainty. Posner's framework emphasizes efficiency as the central concern of legal analysis, asserting that the law should facilitate outcomes that maximize societal economic welfare. From an economic theory of law perspective, the advancements in information technology that have given rise to the digital economy offer substantial gains in efficiency.¹⁹ Technology enables transactions to occur more swiftly, at lower costs, and on a broader scale, thereby contributing to overall economic welfare.

In this regard, regulatory frameworks such as Government Regulation No. 71 of 2019 and Law No. 1 of 2024 provide a legal basis for electronic transactions, fostering the development of efficient markets. These regulations establish a coherent legal framework for market participants, facilitating their operations by mitigating legal risks and reducing the costs associated with legal uncertainty. By providing a structured regulatory environment, these laws contribute to lowering transaction costs, enhancing market efficiency, and thereby supporting the broader goal of economic welfare maximization.

Nevertheless, this perspective must account for potential issues stemming from technological advancements, such as the risk of personal data misuse or losses arising from technological system failures. These issues could result in

¹⁸ Budhijanto, *Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity*. (Bandung: Refika Aditama, 2023), pp. 112-113.

¹⁹ A McGuire, *Law and Economics: N. Mercuro (Ed.)* (Boston: Kluwer Academic Publishers, 1990), [https://doi.org/10.1016/0144-8188\(90\)90025-O](https://doi.org/10.1016/0144-8188(90)90025-O).

significant social costs that legal frameworks must anticipate and address. Consequently, the regulations concerning personal data protection in Government Regulation No. 71 of 2019, alongside the administrative penalties associated with electronic system failures, are designed not only to safeguard individual rights but also to maintain market efficiency. By mitigating potential uncertainties and preventing systemic dysfunction, these regulations aim to uphold a stable and effective market environment.

In relation to electronic contracts as delineated in Government Regulation No. 71 of 2019, the legal framework governing digital contracts should encapsulate the principles of contractual efficiency. The legal provisions should enable the formation of contracts that are expeditious and straightforward between parties, circumventing the complexities of traditional bureaucratic processes. The statutory requirements regarding the validity of electronic contracts, such as the necessity for mutual consent and the legal capacity of the parties involved, can be construed as endorsing the principle of efficiency in transactions. From Posner's economic analysis perspective, there is a critical focus on achieving a balance between flexibility and protection. The law regulating the digital economy must foster innovation and accommodate the rapid pace of technological advancement.

Simultaneously, it must ensure that market mechanisms function effectively and efficiently, thereby mitigating risks associated with system failures that could disrupt market stability. Article 57 of Law No. 1 of 2024, which addresses the nullification of electronic contracts due to technical errors, exemplifies how legal measures are employed to maintain market integrity. This provision ensures that only contracts executed through dependable electronic systems receive legal recognition. From an economic law standpoint, regulations pertaining to electronic transactions and the digital economy are instrumental in creating a stable and efficient market framework. The law, therefore, not only regulates conduct but also functions as a mechanism to enhance the economic value derived from digital market interactions.

C. Cybersecurity in Indonesia: An Analytical Overview

Cybersecurity has emerged as a rapidly expanding sector and has become a pivotal concern for entities across Indonesia. This trend underscores the collective efforts of corporations, individuals, and governmental agencies working together to fortify cybersecurity. Such collaboration is imperative due to the severe repercussions associated with cybersecurity breaches, which can

jeopardize corporate reputations, expose entities to substantial legal liabilities, disrupt business operations significantly, result in the theft of intellectual property, and pose threats to national security. The comprehensive approach to enhancing cybersecurity reflects the understanding that the integrity and stability of both the private and public sectors are critically dependent on robust cybersecurity frameworks.²⁰

The Global Cybersecurity Index (GCI), initially launched in 2015 by the International Telecommunication Union (ITU), is designed to measure the commitment of ITU's 193 member countries to cybersecurity. Its purpose is to assist these nations in identifying areas for improvement and to encourage action by raising awareness about the state of global cybersecurity. According to the National Cyber Security Index (NCSI), Indonesia's cybersecurity index score in 2023 was 63.64 out of 100, marking an increase of 24.68 points from the 38.96 points recorded in 2022. Given the prevalence of cybercrime in Indonesia, cybersecurity must be prioritized. This focus aims to mitigate issues related to personal data breaches and to safeguard Indonesia's digital territory.

Regulating Digital and Cyber Law: A Comparative Analysis of European Union Jurisprudence

The current pace of technological advancement exerts a profound influence on human activities and interactions. This rapid evolution, particularly in communication technology, promises substantial improvements in efficiency and productivity over the long term.²¹ Advances in technology are expected to significantly reduce transportation and communication costs, enhance global logistics and supply chain efficiency, and decrease trade expenses. Collectively, these technological improvements are anticipated to open new market opportunities and stimulate economic growth, thereby contributing to a more dynamic and interconnected global economy.²²

²⁰ Jeff Kosseff, *Cybersecurity Law* (Hoboken, USA: John Wiley & Sons, Inc., 2020).

²¹ Yustina Dhian Novita and Budi Santoso, "Urgensi Pembaharuan Regulasi Perlindungan Konsumen Di Era Bisnis Digital," *Jurnal Pembangunan Hukum Indonesia* 3, no. 1 (2021): 46–58, <https://doi.org/10.14710/jphi.v3i1.46-58>.

²² Syod Ahsanul Islam Ashik, Sahariya Afroje, and Nazmul Hossain, "4th Industrial Revolution: The Beginning of Imagination Age," *Advances in Social Sciences Research Journal* 10, no. 1 (2023): 68–72, <https://doi.org/10.14738/assrj.101.13481>.

The recent advancements in high-tech fields, including computing, electrical engineering, and telecommunications, have been substantial.²³ This rapid technological progress has been accompanied by an increasing public awareness and adoption of more straightforward technological solutions. One notable development is the emergence of Digital Platform Powerplay (DPP), which refers to the use of advanced algorithmic digital platforms. These platforms offer state-of-the-art solutions for managing digital assets by employing sophisticated algorithms to enhance digital activities.²⁴ The adoption of such platforms has markedly improved business operations by streamlining processes and increasing efficiency. However, the proliferation of these platforms also introduces potential adverse effects. The facilitation of transactions through digital platforms on a global scale underscores the advanced nature of current technology, which enables rapid and extensive international commerce. Nevertheless, while the interface for accessing websites may appear consistent across regions such as Europe and Indonesia, significant regulatory and jurisdictional differences remain. This disparity necessitates a nuanced understanding of regional legal frameworks and regulatory environments affecting digital interactions.

In Europe, the practice of presenting users with prominent consent pop-ups—such as "Manage Privacy," "We Value Your Privacy," or "Choose Your Cookie Preferences"—has become standard for accessing web pages, particularly commercial ones. This regulatory approach, driven by the General Data Protection Regulation (GDPR), ensures that users can configure their privacy preferences and exercise their rights to accept or reject cookies based on their specific purposes, including advertising, marketing, and analytics. Such mechanisms afford users the ability to opt out of having their online behavior tracked and utilized for targeted purposes. Users can also reject all cookie consent requests while maintaining access to the website's content. Conversely, this level of privacy control is not uniformly observed in Indonesia. The implementation of similar consent mechanisms remains relatively underdeveloped. In Indonesian e-commerce and commercial websites, users typically do not encounter options for managing privacy settings regarding personal data at the point of access. Although many websites include a "Privacy

²³ Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400–426, <https://doi.org/10.15642/alqanun.2020.23.2.400-426>.

²⁴ Rusdin Tahir et al., *Bisnis Digital (Strategi Administrasi Bisnis Digital Untuk Menghadapi Masa Depan)* (Jambi: PT. Sonpedia Publishing Indonesia, 2023).

Policy" page that outlines how visitor data is handled, the explicit solicitation of user consent is generally absent. This absence indicates a gap in user agency over privacy controls, highlighting a divergence from the more robust privacy protection practices observed in jurisdictions governed by comprehensive data protection regulations like the GDPR.

Privacy is of paramount importance to both individuals and institutions, as the desire to protect privacy is universal and applies to everyone.²⁵ In the Indonesian legal perspective, the focus is on the legal protection and responsibilities applicable to digital platform providers concerning breaches of confidential information and misuse of user data. European Union (EU) law views personal data as any information related to an identified or identifiable living person. Digital or cybersecurity regulations in the EU are implemented through various regulations and laws designed to address cybersecurity threats. The following are key aspects of digital/cyber legal regulation in the European Union:

A. The General Data Protection Regulation

The General Data Protection Regulation (GDPR), established under Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, represents a significant legislative framework within the European Union for the protection of personal data.²⁶ As a central instrument for the harmonization of data protection laws across EU member states, GDPR aims to provide robust safeguards for individuals by regulating the collection, use, and disclosure of personal data. The GDPR encompasses all forms of personal data protection, irrespective of whether such data is stored in written or digital formats. Fundamentally, the GDPR ensures comprehensive protection for all personal data. Personal data is defined under the regulation as information relating to an identified or identifiable individual, which may pertain to personal or professional aspects of life. This includes, but is not limited to, names, addresses, photographs, email addresses, bank account details, medical information, and IP addresses. According to Article 9 of the GDPR, the regulation prohibits the processing of special categories of personal

²⁵ Marike Kondo et al., "Model E-Commerce Untuk Meningkatkan Daya Saing UMKM Dalam Ekosistem Kewirausahaan Digital Di Sulawesi Utara," *Technomedia Journal* 8, no. 2 (2023): 221–34, <https://doi.org/10.33050/tmj.v8i2.2089>.

²⁶ Yahya Ziqra, Mahmul Siregar, and Jelly Leviza, "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online," *Iuris Studia: Jurnal Kajian Hukum* 2, no. 2 (2021): 330–36, <https://doi.org/10.55357/is.v2i2.146>.

data that reveal racial or ethnic origin, religious or philosophical beliefs, genetic data, biometric data, health data, or data concerning an individual's sex life or sexual orientation. This stringent protection reflects the regulation's commitment to safeguarding sensitive personal information against unauthorized disclosure and misuse.

The sanctions outlined in Article 83, paragraph 4 of the General Data Protection Regulation (GDPR) for parties that violate the regulation consist of fines ranging from €10 million to €20 million, or, alternatively, up to 2%–4% of the annual global turnover of the infringing entity. Given that the GDPR is a regulation, the definitive sanctions will be determined by each member state of the European Union. Each EU member state is required to establish at least one public authority responsible for monitoring the implementation of this regulation and providing assistance to data subjects. In the establishment of this authority, the government must ensure transparency, whether through legislative or executive branches. As stipulated in Article 53 of the GDPR, individuals appointed as members of the data protection supervisory authority must possess appropriate qualifications, experience, and expertise in the field of data protection. Therefore, it is imperative that appointments are made judiciously, ensuring that individuals with inadequate understanding of the digital domain are not assigned to these critical roles.

Under the GDPR, personal data may not be processed unless it meets one of the following conditions:

- a) For the legitimate interests pursued by the data controller or by a third party;
- b) For the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller;
- c) To comply with a legal obligation to which the data controller is subject;
- d) For the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into such a contract;
- e) To carry out the data subject's request in relation to contractual matters with the data controller;
- f) To protect the vital interests of the data subject or of another person.

The right to privacy, particularly with respect to personal data, pertains to information that can directly or indirectly identify an individual. Article 4(1) of the General Data Protection Regulation (GDPR) defines personal data as any information relating to an identified or identifiable natural person. This includes identifiers such as names, identification numbers, location data, physical or genetic attributes, as well as data that can be collected through

devices such as smartphones, credit cards, employee IDs, bank accounts, vehicle license plates, and other personal identifiers. If Compared with the context of the Personal Data Protection Act (UU PDP), personal data is described as any information related to an individual that can be identified, either directly or indirectly, through electronic or non-electronic means. The protection of privacy regarding personal data is a fundamental human right and thus necessitates legal safeguarding.

Article 28G(1) of the *Undang-Undang Dasar Negara Republik Indonesia 1945* (UUD 1945) stipulates that every individual is entitled to protection of themselves, their family, their dignity, and their sense of security from threats, thereby mandating the protection of personal data.²⁷ This constitutional provision implies that the state is obligated to uphold and guarantee human rights, including the protection of personal data. Although the article does not explicitly mention privacy, the protection of personal data falls under the broader category of personal rights and individual security.²⁸

B. Cybersecurity Act

The Cybersecurity Act Information and Communications Technology Cybersecurity Certification Regulation (EU) 2019/881 Of the European Parliament and of The Council of 17 April 2019. The European Union's Cybersecurity Act is a significant legislative effort aimed at enhancing cybersecurity across the Union. This Act is designed to prevent and respond to cyber threats while improving the efficiency of resource allocation within the EU. It includes provisions for penalties and enforcement related to violations. Adopted in June 2019 and fully applicable since June 2021, the Cybersecurity Act is a crucial component of EU legislation focused on bolstering cybersecurity across member states. Its primary objectives are to strengthen the European Union Agency for Cybersecurity (ENISA) and to establish a comprehensive cybersecurity certification framework for Information and Communication Technology (ICT) products, services, and processes across the EU. The Act grants ENISA a permanent mandate and expands its resources and responsibilities. ENISA is tasked with:

²⁷ Muhammad Akbar Eka Pradana and Horadin Saragih, "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya," *Innovative Journal of Social Science Research* 4, no. 4 (2024), <https://j-innovative.org/index.php/Innovative/article/view/13476/8935>.

²⁸ Constant Kohler, "The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization," *International Cybersecurity Law Review* 1, no. 1 (2020): 7–12, <https://doi.org/10.1365/s43439-020-00008-1>.

a) *Operational Cooperation*

Enhancing collaboration among EU member states in managing cybersecurity incidents and coordinating responses to large-scale cyber threats.

b) *Certification Framework*

Developing and maintaining a European cybersecurity certification framework that allows for a standardized approach to cybersecurity certification across the EU. This framework is designed to streamline the certification process for businesses, enabling them to obtain certificates that are valid throughout the EU, thereby reducing the compliance burden associated with multiple national certifications.

c) *Cybersecurity Certification Framework*

The EU Cybersecurity Act introduces a risk-based certification framework that establishes general standards for ICT products and services.

d) *Consumer Trust Enhancement*

By ensuring that certified products and services meet high-security standards, the Act aims to foster greater trust among consumers and businesses within the digital market.

e) *Standardization Improvement*

The Act seeks to harmonize existing national certification schemes, which can vary significantly across member states, thereby facilitating easier market access for businesses.

f) *Recent Developments*

In April 2023, the European Commission proposed an amendment to the Act to include certification schemes for managed security services, recognizing the growing importance of these services in the cybersecurity landscape. The amendment aims to enhance the quality and comparability of managed security services across the EU.

The European Union Cybersecurity Act represents a significant step toward a safer digital environment in Europe, addressing the growing risks associated with cyber threats and enhancing the overall resilience of the EU's digital infrastructure. Specifically, Article 58 of the Cybersecurity Act outlines the imposition of penalties that are "effective, proportionate, and dissuasive" for breaches of the regulations. Such penalties may reach up to €20 million or 4% of the global annual turnover of the organization, whichever is greater. The legal

sanctions for violations of the Cybersecurity Act within the EU may entail the following consequences:

a) *Fines*

Countries that violate the Cybersecurity Act may be subject to substantial fines. For instance, technology giants such as Google, Facebook's WhatsApp, and Amazon have been fined tens of millions of euros for breaches related to personal data.

b) *Reputational Damage*

Violating this regulation can tarnish a country's reputation on the international stage. The European Union is recognized as a leader in technology regulation and GDPR, which is part of the broader effort to protect personal data and privacy. A country found in breach of these policies may be perceived as failing to meet the expected standards of data protection.

c) *Challenges in Policy Implementation*

Breaching the Cybersecurity Act can complicate the implementation of policies within the offending country. This regulation is designed to ensure transparency and facilitate the reporting of security breaches involving unauthorized access or disclosure of personal data. Non-compliance with these policies may hinder the ability to report and address security incidents effectively.

d) *Difficulties in Marketing and Exporting*

Countries that violate the Cybersecurity Act may face challenges in marketing and exporting technology products and services, potentially even leading to embargoes. The policy is intended to establish uniform security standards across the EU, and products failing to meet these standards may be barred from the European market.

e) *Erosion of Public Trust*

Breaching this policy may lead to a decline in public trust toward the offending country. The policy aims to safeguard the security, integrity, and confidentiality of information while maintaining stability and confidence in the use of technology. Countries that fail to adhere to these regulations may be perceived as neglecting the digital security of their citizens. Overall, violations of the Cybersecurity Act within the EU can have significant repercussions on reputation, policy implementation, marketing, and public trust.

C. Digital Market Act

The safeguarding of privacy rights within the European Union encompasses not only the GDPR but also a broad spectrum of additional regulatory frameworks. These regulations collectively address the protection of personal rights and the management of cross-border data transfers outside the EU's jurisdiction. The overarching objective of these regulatory instruments is to ensure that privacy and data protection extend to encompass affirmative rights that necessitate proactive engagement from member states. By implementing these diverse regulations, the European Union seeks to foster a secure and efficient environment conducive to digital economic development, while simultaneously maintaining rigorous standards for privacy protection and cybersecurity.

Digital Markets Act (DMA) Regulation (EU) 2022/1925 Of The European Parliament And Of The Council of 14 September 2022, the Digital Markets Act (DMA), enacted by the European Union in 2022, is designed to ensure fairness in the EU digital marketplace.²⁹ This regulation aims to curtail the dominance of large corporations and create an environment that facilitates the entry of new platforms, thereby enhancing competition within the digital market.³⁰ The primary objective of the Digital Markets Act (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022) is to:

a) Creating a Fair Digital Market

The DMA aims to establish a level playing field in the digital realm, particularly for technology companies contending with the significant market dominance of major tech giants.

b) Facilitating Market Entry for New Platforms

The Act is designed to foster an environment conducive to the entry and growth of new platforms, thereby enhancing competition within the digital marketplace.

The subjects regulated under the Digital Markets Act (DMA) primarily include:

a) Major Technology Companies

The DMA targets certain companies, specifically addressing the five major entities dominating internet services commonly referred to as Big Tech (Google, Apple, Meta, Amazon, Microsoft).

b) Gatekeepers

²⁹ Pierre Larouche and Alexandre de Streel, "The European Digital Markets Act: A Revolution Grounded on Traditions," *Journal of European Competition Law & Practice* 12, no. 7 (September 1, 2021): 542–60, <https://doi.org/10.1093/jeclap/lpab066>.

³⁰ Yati Nurhayati, "Regulatory Analysis Digital Markets Act (DMA)," *International Journal of Law, Environment, and Natural Resources* 3, no. 1 (2023): 107–24, <https://doi.org/10.30641/dejure.2021.v21.109->.

These companies are designated as "*gatekeepers*," referring to platform operators with substantial market power.

The principal rules of the Digital Markets Act (DMA) require that companies provide business users with access to their data and ensure that such data can be utilized effectively. Companies must offer European consumers a choice when selecting a web browser or search engine. Furthermore, companies are obligated to submit compliance reports to the European Commission and adhere to all regulations by midnight Brussels time. The impacts and implementation of the European Union's Digital Markets Act are as follows:

- a) The impact of the Digital Markets Act is anticipated to compel large technology companies to comply with these new regulations, which will pose a significant challenge.
- b) The implementation of this Act commenced on May 2, 2023, and the targeted companies are required to adhere to the new rules starting from March 6, 2024.

The Digital Markets Act (DMA) represents a significant and rigorous measure by the European Union to regulate the digital market and ensure that major technology companies adhere to fair and competitive rules. The DMA outlines several provisions addressing violations by gatekeepers. Notably, Article 30 pertains to fines, stipulating that the European Commission may impose fines on gatekeepers for non-compliance with the obligations set forth in the DMA. These fines may not exceed 10% of the gatekeeper's global turnover for the preceding financial year. Furthermore, specific examples of non-compliance include:

- a) Failure to provide the required information or provision of information that is incorrect, incomplete, or misleading.
- b) Failure to comply with notification obligations.
- c) Failure to grant access to data, algorithms, or information regarding testing.
- d) Failure to correct erroneous information or to provide complete information during inspections.
- e) Refusal to submit to inspections.
- f) Failure to comply with obligations imposed by the Commission.
- g) Failure to implement compliance functions.
- h) Failure to adhere to requirements for accessing Commission files.

Under Article 5 of the Digital Markets Act, which addresses User Consent, companies are mandated to seek explicit consent from users before utilizing their data for purposes beyond those for which the data was initially collected. Non-compliance with this stipulation may incur substantial penalties, potentially reaching up to 20% of the gatekeeper's global turnover for the

previous financial year, should the infringement be repeated. Furthermore, Article 30 delineates the regulatory framework for imposing fines. According to this provision, fines can be imposed up to a cap of 10% of the gatekeeper's global turnover for the preceding financial year. In instances of recurrent violations, the penalty may escalate, potentially reaching up to 20% of the gatekeeper's global turnover for the prior financial year. This tiered approach underscores the Digital Markets Act's commitment to enforcing compliance and maintaining rigorous oversight over digital market practices.

In Article 6 of the Digital Markets Act, titled "Ranking and Indexing", it is stipulated that gatekeepers are prohibited from prioritizing their own services over those of third parties in search rankings and indexing. This regulation is designed to promote transparency, fairness, and non-discriminatory practices within the digital marketplace. By ensuring that gatekeepers do not engage in preferential treatment, the Act seeks to create a level playing field for all market participants. Article 7, addressing "Interoperability and Data Access", requires gatekeepers to facilitate interoperability with their services under specific, clearly defined conditions. Interoperability is understood as the ability of various applications and systems to securely and automatically exchange data, transcending geographical, political, or organizational boundaries. This provision is crucial to prevent gatekeepers from creating competitive barriers by restricting access to their platforms, thereby ensuring an open and competitive digital environment. These regulatory measures collectively aim to enforce equitable and transparent business practices among gatekeepers, thereby enhancing contestability and fairness in the digital economy. In contrast, Indonesia's regulatory framework, specifically Law No. 27 of 2022 on Personal Data Protection (UU PDP) and Ministerial Regulation No. 20 of 2016 concerning Personal Data Protection in Electronic Systems, exhibits certain gaps when compared to the European standards embodied in the General Data Protection Regulation (GDPR). Issues such as the precise definition and classification of Personal Data, the standardization of corporate regulatory practices, and the provisions for the notification of data erasure are areas where Indonesian regulations currently lack clarity and comprehensiveness. Consequently, the management of personal data in Indonesia remains inadequately supervised, leading to instances of data breaches and misuse involving Indonesian social media users. This situation underscores the necessity for an update and refinement of Indonesian regulations to align with contemporary standards and effectively safeguard personal data.

The GDPR stands as a seminal regulation in the realm of data management, particularly regarding the erasure of personal data. This

regulation's framework underscores the critical need for reform in Indonesia's legal approach to data erasure. The GDPR's provisions offer a compelling model for enhancing data protection, which could address current deficiencies in Indonesian law. Article 17(3) of the GDPR specifically deals with the notification and mechanism for the erasure of personal data. This provision allows for the deletion of personal data upon user request without necessitating judicial intervention. This contrasts sharply with the Indonesian legal framework, which often requires judicial processes for data erasure, thereby introducing additional complexities and delays. The GDPR's approach ensures that individuals have straightforward mechanisms for requesting data deletion, enhancing both user autonomy and operational transparency. By integrating similar provisions into Indonesian regulations, there could be substantial improvements in data protection practices. Such reforms would not only streamline the data erasure process but also align Indonesia more closely with international standards, thereby strengthening the overall efficacy of personal data protection in the country.

Conclusion

The rapid advancements in technology have led to the widespread integration of electronic media into everyday activities across the Indonesian population. This transformation extends beyond high-tech sectors such as computing to encompass industries like mechanical, chemical, and other fields. These developments have provided significant benefits, particularly in facilitating business operations. However, the increasing reliance on electronic transactions, social media, and digital commerce underscores the urgent need for robust protection of personal data to mitigate the risks of cybercrime. The regulatory framework governing electronic systems and cybersecurity must be interconnected and mutually reinforcing to address these concerns effectively.

Unfortunately, the current state of cybersecurity in Indonesia remains insufficient to support a population that is becoming increasingly proficient with technology. In contrast, the European Union has implemented comprehensive legislative measures to safeguard digital and cyber interests. The General Data Protection Regulation (GDPR), adopted under Regulation (EU) 2016/679, marks a significant advancement in personal data protection. Its primary objective is to enhance data security for EU citizens by establishing stringent guidelines for the collection, processing, and safeguarding of personal data. Additionally, the Digital Markets Act (DMA) was introduced to strengthen the European Union Agency for Cybersecurity (ENISA) and create

a robust cybersecurity certification framework across the EU for Information and Communication Technology (ICT) products, services, and processes. This regulation aims to address the dominance of large technology companies and foster a more competitive environment by facilitating the entry of new platforms.

In light of these developments, it is recommended that Indonesia amend Law No. 11/2008 on Electronic Information and Transactions to foster greater competitiveness. Furthermore, the country should establish a comprehensive cybersecurity certification framework for ICT products, services, and processes, similar to the model implemented by ENISA in the European Union. These steps would enhance Indonesia's cybersecurity landscape and promote a more secure and competitive digital economy.

References

- Anggen Suari, Kadek Rima, and I Made Sarjana. "Menjaga Privasi Di Era Digital: Perlindungan Data Pribadi Di Indonesia." *Jurnal Analisis Hukum* 6, no. 1 (2023): 132–42. <https://doi.org/10.38043/jah.v6i1.4484>.
- APJII. "Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang." Asosiasi Penyelenggara Jasa Internet Indonesia, 2023. <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>.
- Ashik, Syod Ahsanul Islam, Sahariya Afroje, and Nazmul Hossain. "4th Industrial Revolution: The Beginning of Imagination Age." *Advances in Social Sciences Research Journal* 10, no. 1 (2023): 68–72. <https://doi.org/10.14738/assrj.101.13481>.
- Ayu D, Ananthia, Anindyajati Titis, and Abdul Ghoffar. *Perlindungan Hak Privasi Atas Data Diri Di Era Ekonomi Digital*. Jakarta: Pusat Penelitian dan Pengkajian Perkara Mahkamah Konstitusi, 2019.
- Benuf, Kornelius, Siti Mahmudah, and Ery Agus Priyono. "Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia." *Refleksi Hukum: Jurnal Ilmu Hukum* 3, no. 2 (2019): 145–60. <https://doi.org/10.24246/jrh.2019.v3.i2.p145-160>.
- Borges, Cius, Fortes Doutor, Universidade Est, Vrije Universiteit Brussel, Stricto Sensu, Pesquisador Visitante, Vrije Universiteit Brussel, et al. "Perspectivas para o ensino de ciberdireito a partir das novas diretrizes curriculares para os cursos de direito no Brasil: Perspectives for the study of cyber law from the new curricular guidelines for law courses in Brazil." *Revista Jurídica* 01, no. 54 (2019): 639–60.

- <https://doi.org/10.6084/m9.figshare.12093861>.
- Brkan, Maja. "The Essence of the Fundamental Rights to Privacy and Data Protection: Finding the Way through the Maze of the CJEU's Constitutional Reasoning." *German Law Journal* 20, no. 6 (2019): 864–83. <https://doi.org/10.1017/glj.2019.66>.
- Budhijanto, Danrivanto. *Hukum Pelindungan Data Pribadi Di Indonesia: Cyberlaw & Cybersecurity*. Bandung: PT Refika Aditama, 2023.
- Dimitrou, Christos. "Lex Informatica and Legal Regime: Their Relationship." *Electronic Journal*, 2015. <https://doi.org/10.2139/SSRN.2626941>.
- Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400–426. <https://doi.org/10.15642/alqanun.2020.23.2.400-426>.
- Handayanti, Asih. "The Role of Cyber Law in The Use of Technology in Mass Media." *Legal Brief* 11, no. 5 (2022): 2722–4643. <https://doi.org/10.35335/legal.the>.
- Huggins, Michael. "The Right to Privacy: An Argument for A Non-Derivative Right to Privacy." *New York State Bar Association (NYSBA)*. New York University, 2011. <https://doi.org/10.2139/ssrn.2416653>.
- Kohler, Constant. "The EU Cybersecurity Act and European Standards: An Introduction to the Role of European Standardization." *International Cybersecurity Law Review* 1, no. 1 (2020): 7–12. <https://doi.org/10.1365/s43439-020-00008-1>.
- Kondoj, Marike, Herry Langi, Yoice Putung, and Arief Kumaat. "Model E-Commerce Untuk Meningkatkan Daya Saing UMKM Dalam Ekosistem Kewirausahaan Digital Di Sulawesi Utara." *Technomedia Journal* 8, no. 2 (2023): 221–34. <https://doi.org/10.33050/tmj.v8i2.2089>.
- Kosseff, Jeff. *Cybersecurity Law*. Hoboken, USA: John Wiley & Sons, Inc., 2020.
- Larouche, Pierre, and Alexandre de Streel. "The European Digital Markets Act: A Revolution Grounded on Traditions." *Journal of European Competition Law & Practice* 12, no. 7 (September 1, 2021): 542–60. <https://doi.org/10.1093/jeclap/lpab066>.
- Luthfi, Rosihan. "Perlindungan Data Pribadi Sebagai Perwujudan Perlindungan Hak Asasi Manusia." *Jurnal Sosial Teknologi* 2, no. 5 (2022): 431–36. <https://doi.org/10.59188/jurnalsostech.v2i5.336>.
- McGuire, A. *Law and Economics: N. Mercurio (Ed.)*. Boston: Kluwer Academic Publishers, 1990. <https://doi.org/https://doi.org/10.1016/0144->

- 8188(90)90025-O.
- Miller, Nigel. "Cyberlaw — Legal Issues Online." *Computer Audit Update*, no. 12 (1995): 4–9. [https://doi.org/https://doi.org/10.1016/S0960-2593\(00\)80061-0](https://doi.org/https://doi.org/10.1016/S0960-2593(00)80061-0).
- Mutiara, Upik, and Romi Maulana. "Perlindungan Data Pribadi Sebagai Bagian Dari Hak Asasi Manusia Atas Perlindungan Diri Pribadi." *Indonesian Journal of Law and Policy Studies* 1, no. 1 (2020): 42. <https://doi.org/10.31000/ijlp.v1i1.2648>.
- Novita, Yustina Dhian, and Budi Santoso. "Urgensi Pembaharuan Regulasi Perlindungan Konsumen Di Era Bisnis Digital." *Jurnal Pembangunan Hukum Indonesia* 3, no. 1 (2021): 46–58. <https://doi.org/10.14710/jphi.v3i1.46-58>.
- Nurhayati, Yati. "Regulatory Analysis Digital Markets Act (DMA)." *International Journal of Law, Environment, and Natural Resources* 3, no. 1 (2023): 107–24. <https://doi.org/10.30641/dejure.2021.v21.109->.
- Pfisterer, Valentin M. "The Right to Privacy—a Fundamental Right in Search of Its Identity: Uncovering the CJEU's Flawed Concept of the Right to Privacy." *German Law Journal* 20, no. 5 (2019): 722–33. <https://doi.org/10.1017/glj.2019.57>.
- Pradana, Muhammad Akbar Eka, and Horadin Saragih. "Prinsip Akuntabilitas Dalam Undang-Undang Perlindungan Data Pribadi Terhadap GDPR Dan Akibat Hukumnya." *Innovative Journal of Social Science Research* 4, no. 4 (2024). <https://j-innovative.org/index.php/Innovative/article/view/13476/8935>.
- Purnama, Thiara Dewi, and Abdurrahman Alhakim. "Pentingnya UU Perlindungan Data Pribadi Sebagai Bentuk Perlindungan Hukum Terhadap Privasi Di Indonesia." *E-Journal Komunitas Yustisia* 4, no. 3 (2021): 273–83. <https://ejournal.undiksha.ac.id/index.php/jatayu/article/view/44370/21087>.
- Ramdhani, Fahmi Ali. "Lex Informatica Theory Approach as An Architecture To Prevent And Handle Hate Speech In Cyberspace," *Tianjin Daxue Xuebao (Ziran Kexue yu Gongcheng Jishu Ban)/ Journal of Tianjin University Science and Technology* 56, no. 10 (2023): 231–42. <https://doi.org/10.5281/zenodo.8424414>.
- Saly, Jeane Neltje, Halena Artamevia, Kendelif Kheista, Barnabas Juni Saputra Gulo, Evellyn Abigael Rhemrev, and Michelle Christie. "Analisis Perlindungan Data Pribadi Terkait UU No.27 Tahun 2022." *Jurnal Serina Sosial Humaniora* 1, no. 3 (2023): 145–53.

<https://doi.org/10.24912/jssh.v1i3.28615153>.

Dhifa Nadhira Syadzwina, Dominikus Rato, and Bayu Dwi Anggono. "The Legal Position of Limited Partnership in Indonesia through the Perspective of the Philosophy of Utilitarianism." *International Journal of Social Science and Education Research Studies* 03, no. 11 (2023): 2247–57. <https://doi.org/10.55677/ijssers/v03i11y2023-11>.

Tahir, Rusdin, Ratih Purbasari, Rony Sandra Yofa Zebua, and Chandra Hendriyani. *Bisnis Digital (Strategi Administrasi Bisnis Digital Untuk Menghadapi Masa Depan)*. Jambi: PT. Sonpedia Publishing Indonesia, 2023.

Tapscott, Don. *The Digital Economy: Promise and Peril in the Age of Networked Intelligence*. New York: McGraw-Hill, 1995.

Tzanou, Maria. "Data Protection as a Fundamental Right next to Privacy? 'Reconstructing' a Not so New Right." *International Data Privacy Law* 3, no. 2 (May 1, 2013): 88–99. <https://doi.org/10.1093/idpl/ipt004>.

Ziqra, Yahya, Mahmud Siregar, and Jelly Leviza. "Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online." *Iuris Studia: Jurnal Kajian Hukum* 2, no. 2 (2021): 330–36. <https://doi.org/10.55357/is.v2i2.146>.

Acknowledgment

None

Funding Information

None

Conflicting Interest Statement

The author(s) stated that this work is original and has not been previously published in another journal or publication. The author(s) also declared that there is no conflict of interest in the publication of this article.

History of Article

Submitted : March 21, 2024

Revised : June 11, 2024; September 30, 2024

Accepted : October 25, 2024

Published : November 30, 2024