INVEST: Journal of Sharia and Economic Law
Vol. 4, No. 2, December 2024 (pp. 292-316)

E-ISSN 2776-4354
P-ISSN 2776-4982

ESTABLISHING A PERSONAL DATA PROTECTION AGENCY FOR E-COMMERCE IN INDONESIA: LEGAL FRAMEWORK AND IMPLEMENTATION CHALLENGES

Bilqis Laila Nuzul Sa'adah[1], Sukarmi[2], Reka Dewantara[3]

[12] Faculty of Law, University of Brawijaya, Indonesia
Email: bilqislailaa@student.ub.ac.id

DOI: 10.21154/invest.v4i2.10031

Received: 2024-10-24	*Revised: 2024-12-05*	*Approved: 2024-12-25*

Abstract: The rapid growth of e-commerce in Indonesia has led to a significant increase in the collection and processing of personal data, raising concerns regarding data security and privacy rights. This study analyzes the urgency of establishing a Personal Data Protection Agency (LPDP) specifically for e-commerce users in Indonesia, considering the increasing risks to personal data in the digital marketplace. This research focuses on addressing the limitations of the current legal framework, particularly the gaps in the Indonesian Personal Data Protection Law (UU No. 27 of 2022), and proposes an independent body with clear authority to regulate, monitor, and enforce data protection standards. This study employs a qualitative approach using normative legal analysis to evaluate existing regulations and assess the evolving needs of the e-commerce sector. The findings suggest that the absence of detailed implementation regulations and lack of a specific regulatory body create significant legal uncertainties, exposing users to potential data breaches. Establishing the LPDP is expected to strengthen data protection measures, enhance consumer trust, and provide legal certainty in Indonesia's digital economy. The proposed structure of the LPDP includes directorates for policy and regulation, supervision and audits, law enforcement, and public education and awareness. The implementation of effective personal data protection policies requires a comprehensive and coordinated approach, with the LPDP having sufficient authority and resources to perform its duties. This study highlights the importance of establishing an independent regulatory body to ensure the protection of personal data and privacy rights in Indonesia's rapidly expanding e-commerce sector.

Keywords: *Personal Data Protection, E-commerce, Legal Framework*

Abstrak: Pesatnya pertumbuhan e-commerce di Indonesia telah menyebabkan peningkatan yang signifikan dalam pengumpulan dan pemrosesan data pribadi, sehingga menimbulkan kekhawatiran tentang keamanan data dan hak-hak privasi. Penelitian ini bertujuan untuk menganalisis urgensi pembentukan Lembaga Perlindungan Data Pribadi (LPDP) khusus untuk pengguna e-commerce di Indonesia, mengingat meningkatnya risiko data pribadi di pasar digital. Penelitian ini berfokus pada upaya untuk mengatasi keterbatasan kerangka hukum yang ada saat ini, khususnya kesenjangan dalam Undang-Undang Perlindungan Data Pribadi (UU No. 27 Tahun 2022), dan mengusulkan sebuah badan independen dengan wewenang yang jelas untuk mengatur, memantau, dan menegakkan standar perlindungan data. Penelitian ini menggunakan pendekatan kualitatif dengan menggunakan analisis normatif hukum untuk mengevaluasi peraturan yang ada dan menilai kebutuhan yang berkembang di sektor e-commerce. Temuan penelitian menunjukkan bahwa tidak adanya peraturan pelaksanaan yang terperinci dan kurangnya badan pengawas khusus menciptakan ketidakpastian hukum yang signifikan, yang membuat pengguna terekspos pada potensi pelanggaran data. Pembentukan LPDP diharapkan dapat memperkuat langkah-langkah

perlindungan data, meningkatkan kepercayaan konsumen, dan memberikan kepastian hukum dalam ekonomi digital Indonesia. Struktur LPDP yang diusulkan mencakup perlunya direktorat untuk kebijakan dan regulasi, pengawasan dan audit, penegakan hukum, serta edukasi dan kesadaran publik. Penerapan kebijakan perlindungan data pribadi yang efektif membutuhkan pendekatan yang komprehensif dan terkoordinasi, dengan LPDP memiliki wewenang dan sumber daya yang memadai untuk melaksanakan tugasnya. Studi ini menyoroti pentingnya pembentukan badan pengawas independen untuk memastikan perlindungan data pribadi dan hak-hak privasi di sektor e-commerce yang berkembang pesat di Indonesia.

Kata kunci**:** *Perlindungan Data Pribadi, E-commerce, Kerangka Hukum*

INTRODUCTION

In today's digital era, the rise of e-commerce activities in Indonesia has led to a massive increase in the collection of consumer data. E-commerce platforms, which are rapidly growing, routinely gather extensive personal data, ranging from demographic information to users' financial transaction details.[1] While this practice offers benefits in terms of service personalization and efficiency, it also raises critical questions regarding the boundaries and usage of such data.

The discourse on privacy rights and data security has become increasingly relevant in light of numerous surfaced data breaches, highlighting the vulnerabilities of the existing systems.[2] These concerns are not limited to the technical aspects of data security but also emphasize the need for a robust legal framework to protect individual rights.

Although Indonesia enacted Law Number 19 of 2016, an amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (hereafter referred to as the ITE Law), which covers some aspects of data protection, this regulation is still deemed insufficient to address the specific needs arising from the dynamics of e-commerce, as stated by Muhammad Nur Aldiansyah.[3]

---

[1] Rita Rahayu and John Day, 'E-Commerce Adoption by SMEs in Developing Countries: Evidence from Indonesia', *Eurasian Business Review* 7, no. 1 (April 2017): 25–41, https://doi.org/10.1007/s40821-016-0044-6.

[2] Muhamad Nur Aldiyansyah, Fatya Alty Amalia, and Gundur Leo, 'Understanding the Effect of E-Commerce Security Towards Loyalty': (2nd International Seminar of Science and Applied Technology (ISSAT 2021), Bandung, Indonesia, 2021), https://doi.org/10.2991/aer.k.211106.093.

[3] Muhammad Abdurrohim, Indah Kumalasari, and Fathur Rosy, 'The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective', *Jurnal Hubungan Internasional* 11, no. 2 (19 September 2022): 13–23, https://doi.org/10.18196/jhi.v11i2.14361.

Globally, data privacy issues have garnered serious attention through strict regulations such as the General Data Protection Regulation (GDPR) implemented by the European Union. The GDPR is considered the gold standard for personal data protection, providing an important example of how effective regulation can be applied.[4] This regulation emphasizes transparency, accountability of data controllers, and greater control over consumers' personal data. This includes the right to be informed about data usage, the right to delete data, and the right to withdraw consent.[5] The protection of personal data is closely linked to the right to privacy, which is recognized as a fundamental human right. The right to privacy is enshrined in various international human rights instruments, including Article 12 of the Universal Declaration of Human Rights (UDHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR), which guarantees that every individual's right to be protected from unauthorized interference with their privacy, including in the context of personal information. In the digital era, privacy violations through the misuse of personal data have become an increasingly real threat, especially in the e-commerce sector, where consumer data are collected, stored, and processed in large volumes. Given the high risk to individuals' privacy, an independent agency such as the Personal Data Protection Agency (LPDP) is essential, as it would have the authority and capacity to oversee and enforce personal data protection without being influenced by specific political or economic interests.

The establishment of an independent agency, such as the LPDP, would provide greater assurance in safeguarding e-commerce consumers' privacy rights, as the primary role of this agency is to regulate, monitor, and address violations objectively. The independence of this agency allows the LPDP to carry out its duties with a primary focus on protecting consumers' human rights, free from potential interference or conflicts of interest that could arise if they were under the direct control of ministries or other parties with commercial interests. Moreover, independent agencies tend to have higher credibility and public trust, which encourages e-commerce companies to comply with established regulations.

At the international level, high standards of data protection have been adopted through the General Data Protection Regulation (GDPR) implemented by the

[4] Mahsa Shabani and Pascal Borry, 'Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation', *European Journal of Human Genetics* 26, no. 2 (February 2018): 149–56, https://doi.org/10.1038/s41431-017-0045-7.

[5] Gauthier Chassang, 'The Impact of the EU General Data Protection Regulation on Scientific Research', *Ecancermedicalscience* 11 (3 January 2017), https://doi.org/10.3332/ecancer.2017.709.

European Union. The GDPR grants individuals important rights, such as the right to access and the right to know how their personal data are used, as well as the right to rectify or delete data if it is no longer relevant or necessary. This regulation also includes strong supervisory mechanisms where independent data protection authorities in each EU member state are empowered to audit, monitor, and enforce compliance with personal data regulations.[6] By referring to GDPR standards, the establishment of a Personal Data Protection Agency (LPDP) with similar authority in Indonesia could be a significant step towards enhancing the privacy rights of e-commerce consumers, providing individuals with clear access to manage their data, and ensuring stringent oversight of companies that process personal data.

Currently, Indonesia is preparing for this, as mandated by Article 58 paragraph (3) of the Personal Data Protection Law (UU PDP), which fully delegates this responsibility to the president. Consequently, the Ministry of Communication and Informatics, as the relevant ministry, is still drafting regulations, including the establishment of Personal Data Protection.[7] Authority. However, it is anticipated that this authority will operate similarly to the National Agency of Drug and Food Control (BPOM) and the Central Bureau of Statistics (BPS).

In addition to legal protection and independent oversight, technical data security is essential for protecting e-commerce users' personal data. Technical security standards, such as encryption, are key elements for safeguarding data from unauthorized access. Data encryption ensures that sensitive information, such as personal and financial transaction data, remains secure, even if a breach or unauthorized access occurs. According to research by Tikkinen-Piri, Rohunen, and Markkula, robust encryption and other security protocols, such as multi-factor authentication and firewalls, significantly reduce the risk of data breaches.[8] The GDPR also requires companies to implement adequate technical and organizational security measures as a form of accountability in managing personal data. By referring to these international standards, Indonesia must ensure that e-commerce companies

[6] Michelle Goddard, 'The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact', *International Journal of Market Research* 59, no. 6 (November 2017): 705, https://doi.org/10.2501/IJMR-2017-050.

[7] https://www.cnnindonesia.com/teknologi/20240129132212-192-1055704/ kominfo-sebut-lembaga-pengawas-pdp-bakal-dibentuk-pertengahan-2024

[8] Christina Tikkinen-Piri, Anna Rohunen, and Jouni Markkula, 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies', *Computer Law & Security Review* 34, no. 1 (February 2018): 135, https://doi.org/10.1016/j.clsr.2017.05.015.

implement advanced security technologies to protect the integrity of user data. Strong security standards not only protect consumers, but also reinforce public trust in Indonesia's digital ecosystem, which is essential for supporting the growth of the e-commerce sector in the digital age.

Currently, no specific regulations comprehensively address consumer data protection in the digital marketplace. This absence creates significant risks not only for users but also for the entire e-commerce ecosystem, which relies on consumer trust for growth and sustainability. The problem is further complicated by the fact that e-commerce transactions often involve multiple parties and cross-border data transfers, requiring regulations that are not only nationally effective but also compatible with international standards.[9] Inadequate data security and inconsistent privacy policies across platforms can lead to misuse of personal data and an increase in online fraud cases.

The legal issue of personal data protection in Indonesia stems from the ambiguity and incompleteness of several articles in Law Number 27 of 2022 on Personal Data Protection (UU PDP), as well as the absence of detailed implementation regulations. For example, Article 35, which regulates the consent of data subjects, does not clearly explain the mechanism for obtaining valid consent, which leads to uncertainty in its implementation. Additionally, Article 57, which outlines the obligations of data controllers to maintain confidentiality, requires detailed implementation regulations to ensure effective compliance. These shortcomings hinder the optimal protection of data subjects' rights and necessitate the urgent issuance of clearer regulations.

To address these legal challenges and examine the current state of personal data protection in Indonesia, this study employed normative legal research. This approach conceptualizes law as what is written in legislation (law in books) or as a set of norms or standards that guide human behavior deemed appropriate. The author's research focuses on examining the legal protection framework provided through various regulations issued by the Government of the Republic of Indonesia, particularly regarding the data security and privacy of e-commerce consumers.

[9] Ömer Faruk Derindağ, 'Rise of Cross-Border E-Commerce: A Systematic Literature Review', *Journal of Applied And Theoretical Social Sciences* 4, no. 3 (11 September 2022): 352–72, https://doi.org/10.37241/jatss.2022.71.

In the context of this research, a normative approach was applied to analyze the existing legal framework. The normative approach in this study focuses on an in-depth analysis of legislative texts, particularly the Personal Data Protection Act (UU PDP) and the Electronic Information and Transactions Act (UU ITE). The primary purpose of using this normative method is to evaluate the extent to which existing regulations are adequate for protecting users' personal data, especially in the context of e-commerce. Through this analysis, this study will assess the consistency between articles within the UU PDP and UU ITE, as well as the comprehensiveness of these regulations in addressing the need for personal data protection in the digital era. This method also aims to evaluate the effectiveness of the current legal provisions, specifically, whether they are robust enough to counteract various threats to user privacy and data security. This approach is expected to reveal potential weaknesses and strengths of existing regulations, enabling more targeted and evidence-based recommendations.

The normative method in this research is used to assess whether the Personal Data Protection Act (UU PDP) can provide sufficient legal certainty. The principle of legal certainty aims to ensure that existing regulations do not create ambiguity in their application so that business actors can clearly follow the rules and consumers can feel secure regarding the protection of their personal data. Through this evaluation, this study aims to identify the extent to which the UU PDP provides clarity and consistency in protecting personal data, thus ensuring that the regulation can be effectively implemented in a dynamic e-commerce environment.

DISCUSSION

1.1 Analysis of Data Weaknesses in E-Commerce

The use of e-commerce in Indonesia has experienced significant growth in the continuously evolving digital era. The ease of access and various benefits offered by e-commerce platforms have encouraged the public to engage in online transactions more frequently. This rapid growth has had a positive impact on Indonesia's digital economy; however, it also presents new challenges, especially regarding the protection of personal data for e-commerce users.[10] Personal data protection in e-

[10] Muhammad Prakoso Aji, 'Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]', *Jurnal Politica Dinamika Masalah Politik*

commerce has become an increasingly urgent issue in the current digital age. As technology and Internet adoption rise, e-commerce in Indonesia has seen rapid growth, transforming how consumers interact with markets and conduct commercial transactions. E-commerce platforms collect various types of personal data from users, ranging from demographic information and shopping preferences to financial transaction details. These data are highly valuable to e-commerce companies, as they enable service personalization, more accurate ad targeting, and improved operational efficiency. However, the collection and use of personal data poses significant challenges related to consumer privacy and data security.

Personal data protection is a fundamental issue because it concerns the privacy rights of individuals, which are guaranteed by various international and national legal instruments. In Indonesia, attention to this issue has increased owing to several data breaches that have occurred, highlighting the weaknesses of existing systems for protecting users' personal data. Data breaches not only harm individuals but can also damage a company's reputation and erode public trust in the e-commerce ecosystem. Therefore, effective regulations and strict law enforcement are essential to ensure that the personal data of e-commerce users are well protected.[11]

Indonesia has several regulations related to personal data protection, such as Law Number 19 of 2016, which is an amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law), as well as Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). However, these regulations are considered insufficient to address the specific needs arising from e-commerce dynamics. For instance, the ITE Law focuses more on regulating electronic transactions and communications in general without paying special attention to personal data protection in the context of e-commerce. The provisions in the ITE Law that relate to personal data tend to be general and lack detailed guidance on the mechanisms for collecting, managing, and using personal data from e-commerce platforms.[12]

Dalam Negeri Dan Hubungan Internasional 13, no. 2 (4 January 2023): 222–38, https://doi.org/10.22212/jp.v13i2.3299.

[11] Radi P. Romansky et al., 'Challenges of the Digital Age for Privacy and Personal Data Protection', *Mathematical Biosciences and Engineering* 17, no. 5 (2020): 5288–5303, https://doi.org/10.3934/mbe.2020286.

[12] Samuel Christian Salim and Jeane Neltje, 'Analysis of Legal Protection Towards Personal Data in E-Commerce': (3rd Tarumanagara International Conference on the Applications of Social Sciences

One of the important aspects that remains under-regulated in ITE Law and the PDP Law is the mechanism for effective oversight and law enforcement. Without clear and firm mechanisms, existing regulations tend to lack sufficient impetus to ensure compliance from the parties involved in the management of personal data. This can be seen from frequent data breach cases that have not received adequate handling, either in terms of investigation or sanction enforcement. In several countries, such as the European Union, independent institutions have been established to oversee and enforce personal data protection regulations. Such institutions are empowered to conduct audits, impose sanctions, and ensure that citizens' personal data rights are well-protected.[13]

Additionally, the ITE Law and PDP Law have yet to specifically regulate the management of data involving third parties, such as cloud service providers and other third-party entities that are often involved in the e-commerce data management chain. In an e-commerce ecosystem, personal data are often processed and stored by various parties, adding complexity to the management and protection of these data. Without clear regulations regarding the responsibilities and obligations of each party involved, the risk of data breach and misuse increases.[14]

The protection of privacy rights has become increasingly urgent in the digital era as privacy is recognized as a fundamental human right in both international and national law. Internationally, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) guarantee individuals' rights to privacy, which extends to safeguarding personal data. Privacy rights empower individuals to maintain control over their personal information, which is essential for preserving personal freedom amid rapid digitalization.[15]

The protection of privacy rights has become increasingly urgent in the digital era, as privacy is recognized as a fundamental human right in both international and national legal frameworks. The rapid development of technology has led to

---

and Humanities (TICASH 2021), Jakarta, Indonesia, 2022), https://doi.org/10.2991/assehr.k.220404.101.

[13] Zuboff and Shoshana, *The Age of Surveillance Capitalism Social Theory Re-Wired.* (England: Routledge, 2023).

[14] Tamara Dinev et al., 'Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts', *European Journal of Information Systems* 22, no. 3 (May 2013): 295–316, https://doi.org/10.1057/ejis.2012.23.

[15] Alan F. Westin, 'Social and Political Dimensions of Privacy', *Journal of Social Issues* 59, no. 2 (July 2003): 433, https://doi.org/10.1111/1540-4560.00072.

unprecedented levels of personal data collection and processing, often lacking clear guidelines on how these data are used or protected. In this context, privacy is not only a matter of individual autonomy, but also a vital component of human dignity and security.

Internationally, the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) enshrine the right to privacy, which extends to safeguarding personal data in the digital age. Article 12 of the UDHR and Article 17 of the ICCPR guarantee individuals' protection from arbitrary interference with their privacy, family, home, and correspondence. These provisions underscore privacy as a universal right, fundamental to human dignity and personal security, and stress that any limitation on this right must be necessary, proportionate, and in accordance with law.

Privacy rights, particularly in the context of data protection, empower individuals to maintain control over their personal information—a critical aspect of autonomy and personal freedom amid rapid digitalization. This control is essential not only to prevent abuse of personal information but also to foster a sense of security and trust in digital environments. As individuals increasingly engage in online activities such as e-commerce, social media, and digital communications, they face heightened risks of their data being exploited or mishandled. These risks make it essential to establish legal protections that are adaptive to technological advancements because privacy violations in the digital space can lead to consequences ranging from financial fraud and identity theft to discrimination and psychological harm.

One concrete example of this weakness is the data breach incident that occurred on one of Indonesia's largest e-commerce platforms, Tokopedia in 2020. In May 2020, more than 91 million Tokopedia user data were reported to have been leaked and traded on a dark web forum. The leaked data included sensitive information, such as usernames, email addresses, phone numbers, and hashed passwords. This incident raised serious concerns regarding how personal data are managed and protected by e-commerce platforms in Indonesia.[16] In the case of Tokopedia, although the company stated that users' passwords were hashed and no payment information was leaked, the incident still revealed weaknesses in the data security systems. The inability to

[16] CNN Indonesia, 'Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual', 2020, https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

prevent unauthorized access and large-scale data breaches demonstrates that the obligation of electronic system providers to maintain data confidentiality, as stipulated in the ITE Law, does not provide sufficient protection.

The ITE Law requires electronic system providers to ensure the confidentiality, integrity, and availability of the personal data they manage. However, this law does not provide specific guidelines on the technical and organizational steps that electronic system providers must take to fulfill these obligations. For example, the ITE Law does not provide detailed explanations of the use of encryption, regular security audits, risk assessments, or security incident management. As a result, electronic system providers may lack clear guidance on how to implement protective measures effectively.

The absence of clear operational guidelines in the ITE Law also leaves many electronic system providers, especially small- and medium-sized ones, confused about how to fulfill their obligations regarding personal data protection. Without specific guidance and strict enforcement mechanisms, many companies may fail to implement adequate protective measures, ultimately increasing the risk of data breach.

From an international perspective, we can compare the Tokopedia case with the data breach incident involving the U.S.-based e-commerce company, eBay, in 2014. In May 2014, eBay announced that 145 million users' personal data had been hacked. The stolen data included usernames, encrypted passwords, email addresses, physical addresses, phone numbers, and birth dates. The attack was carried out through compromised employee accounts that provided access to the company's network.

Similar to Tokopedia, eBay has also faced heavy criticism for its failure to protect user data. However, the key difference lies in the response and the available enforcement mechanisms. Under the General Data Protection Regulation (GDPR) in effect in the European Union, companies such as eBay are required to notify data breaches to supervisory authorities within 72 h and to affected individuals without undue delay. Furthermore, the GDPR imposes strict penalties for violations, including fines of up to 20 million euros or 4% of the company's global annual revenue, whichever is higher.[17]

[17] CNBC, 'Hackers Raid eBay in Historic Breach, Access 145M Records', 2014, https://www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html.

1.2 Risks and Impact of Data Breaches

A data breach is an incident in which personal information that should be kept confidential, such as names, addresses, phone numbers, financial information, and other sensitive data, is accessed, used, or disseminated without permission from unauthorized parties. This incident can occur owing to various factors, including cyber-attacks, human negligence, or weaknesses in information technology security systems. In the current digital era, data breaches pose a serious threat because of the high volume of data collected and stored by various entities ranging from e-commerce companies and financial institutions to government agencies. Leaked personal data can be used for various illegal activities such as identity theft, financial fraud, and other cybercrimes.[18]

According to a report by IBM Security, the average global cost of a data breach in 2021 was USD 4.24 million per incident, representing a 10% increase from the previous year. The report also revealed that the average time to identify and address a data breach was 287 days, indicating how slow the incident response process is in many organizations.[19] In Indonesia, data breaches continue to rise, along with the rapid growth of the digital and e-commerce sectors. Data from the Indonesian Internet Service Providers Association (APJII) showed that by 2022, more than 50 million user data from various digital platforms were reported to have been breached, representing a significant increase compared to previous years.[20]

Data breaches not only cause financial losses, but also damage the reputation and public trust of the organization that experienced the incident. User trust is a highly valuable asset for e-commerce companies. When user data are leaked, they are likely to lose trust and switch to other platforms that they perceive as more secure. A study conducted by the Ponemon Institute found that 65% of consumers lost trust in

[18] Ilsun You et al., 'Innovative Security Technologies against Insider Threats and Data Leakage', *International Journal of Computer Mathematics* 93, no. 2 (February 2016): 236–38, https://doi.org/10.1080/00207160.2015.1044784.

[19] IBM Security, 'Cost of a Data Breach 2024 | IBM', 2020, https://www.ibm.com/reports/data-breach.

[20] APJII, 'Kasus Data Pribadi Yang Selalu Bocor' (Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia, 2021), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://apjii.or.id/assets/media/buletin_apjii_edisi_94_-_september_2021_bulletin.pdf.

a company after a data breach, and 31% of them terminated their business relationship with the company.[21]

Vulnerability to data breaches is exacerbated by the fact that many organizations still fail to prioritize investment in adequate security technology and employee training on best practices in data management. According to a report by Cybersecurity Ventures, global spending on cybersecurity is expected to reach USD 1 trillion by 2025, yet many organizations still do not realize the importance of this investment in protecting their digital assets.[22] In Indonesia, many small and medium-sized enterprises (SMEs) still face significant challenges in allocating budgets for cybersecurity, making them more vulnerable to cyber-attacks and data breach.

Data breaches have a significant direct impact on individuals, especially when sensitive personal information falls into the wrong category. One of the primary risks is identity theft, in which cybercriminals use leaked personal information to impersonate legitimate individuals for fraudulent purposes. According to a report from the Identity Theft Resource Center, more than 1.4 million cases of identity theft were reported in the United States in 2021, and this trend is showing an annual increase.[23] Identity theft can cause significant financial losses for victims, including debts incurred in their names and lower credit scores, which can affect their ability to obtain loans or mortgages in the future.

In addition to identity theft, financial fraud is another serious risk faced by individuals as a result of data breach. Criminals can use information such as credit card numbers, bank account details, and login credentials to conduct illegal transactions or access victims' bank accounts. A study conducted by Javelin Strategy and Research revealed that losses due to financial fraud in the United States amounted to more than $16 billion in 2020.[24] This fraud not only results in direct financial losses

---

[21] Thales Group, 'Lack of Consumer Trust across Industries to Protect Their Personal Data, New Research from Thales Has Revealed | Thales Group', 2021, https://www.thalesgroup.com/en/countries-europe/romania/press_release/lack-consumer-trust-across-industries-protect-their-personal.

[22] Ventures and Cybersecurity, 'Cybersecurity Jobs Report' (Herjavec Group 1, 2017).

[23] Ensign Infosecurity, 'Cyber Threat Landscape Report 2024', accessed 31 July 2024, https://www.ensigninfosecurity.com/resources/threat-insights/cyber-threat-landscape-report-2024?utm_source=google&utm_medium=cpc&utm_campaign=cti_report_2024&gad_source=1&gclid=Cj0KCQjwwae1BhC_ARIsAK4Jfrzrw_y4mvCoLNXpkwMqDmLX6KKDasvKBgUvIqjvpBv0IOcOl4oAslUaAuxTEALw_wcB.

[24] Javelin, 'Identity Fraud Study | Javelin', 2021, https://www.javelinstrategy.com/annual-identity-fraud-study.

but also requires significant time and effort for victims to resolve the issue with financial institutions and recover lost funds.

Privacy violations are a serious consequence of data breaches. Sensitive personal information, such as medical records, criminal history, or personal preferences, can be used to harm individuals. These privacy violations can lead to psychological trauma, embarrassment, and other negative effects on an individual's social and professional life. For instance, a medical data breach can reveal confidential health conditions, which may affect personal relationships and job opportunities for victims. According to a report from the Privacy Rights Clearinghouse, medical data breaches have increased by more than 25% between 2019 and 2020, highlighting a growing threat in this sector.[25]

Data breaches not only impact individuals but also pose significant risks to companies that experience violations. One of the main risks is substantial financial loss. According to a report by IBM Security, the average global cost of a data breach in 2021 was USD 4.24 million per incident, an increase of 10% from the previous year.[26] These costs include investigation and recovery expenses, compensation for victims, and repairs to the affected security systems. In addition, companies may face fines from regulators if found in violation of data protection laws such as the General Data Protection Regulation (GDPR) in the European Union, which can impose fines of up to 20 million euros or 4% of the company's global annual revenue, whichever is greater.

Reputational damage is another significant risk for companies that experience data breach. Customer trust is an asset in business, particularly in the e-commerce sector, which relies heavily on users' personal data. A data breach can erode this trust, causing customers to abandon platforms deemed unsafe and to switch to competitors. A study conducted by the Ponemon Institute found that 65% of consumers lost trust in a company after a data breach, and 31% ended their business relationship with the company. Reputational damage can have long-term effects, hindering business growth and leading to a significant decline in revenue.

[25] Privacy Rights, 'Data Breach Chronology | Privacy Rights Clearinghouse', 2020, https://privacyrights.org/data-breaches.

[26] IBM Security, 'Cost of a Data Breach 2024 | IBM'.

1.3 Formulation of Regulation Regarding the Establishment of a Personal Data Protection Agency to Enhance Protection for E-commerce Users

The structure of the Personal Data Protection Agency (LPDP) should be designed as an independent institution that is not under the direct control of ministries or police. The independence of this agency is crucial to ensuring that the LPDP can carry out its functions without political or bureaucratic pressure, which could hinder its effectiveness. However, the LPDP must have a close working relationship with the Ministry of Communication and Informatics (Kominfo) to ensure policy and regulatory synchronization, as well as law enforcement for effective law enforcement.

Establishing the Personal Data Protection Agency (LPDP) in Indonesia as an independent entity is a critical step toward ensuring effective and comprehensive personal data protection. One of the main reasons the LPDP should be structured as an independent agency is to guarantee independence in supervision and law enforcement. This independence is essential for the LPDP to operate without political pressure or particular interests that may hinder its function of oversight. According to Bennett and Raab, independent agencies tend to be more effective in conducting oversight because they have autonomy and freedom from external interference.[27] This enables the LPDP to enforce personal data protection regulations consistently and fairly.

As independent agencies, LPDP should be structured to operate with high transparency and accountability. This includes publishing annual reports on their activities and findings as well as providing incident reporting mechanisms accessible to the public. Transparency is important for building public trust and ensuring that an agency is accountable for its actions. Research by Fung states that transparency and accountability are key elements in ensuring the effectiveness of public policy, including personal data protection. The LPDP, with a dedicated Directorate for public education and awareness, can play a crucial role in enhancing the public's understanding of their rights regarding personal data and how to protect it.[28]

Based on the above reasons, the establishment of the Personal Data Protection Agency (LPDP) as an independent entity with a clear organizational structure and

[27] Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, 1st ed. (Routledge, 2017), https://doi.org/10.4324/9781315199269.

[28] Archon Fung, Mary Graham, and David Weil, *Full Disclosure: The Perils and Promise of Transparency* (Inggris: Cambridge University Press, 2007).

adequate resources is necessary to ensure effective personal data protection in Indonesia. Independence, better coordination, specialized expertise, transparency, accountability, and increased public awareness and education are factors that support the effectiveness of this agency in addressing the challenges of the current digital era.

The main difference between the Personal Data Protection Agency (LPDP) and the National Data Center (PDNS) lies in their primary focus and responsibilities. The LPDP aims to oversee and enforce personal data protection regulations as well as raise public awareness and education on personal data rights. The LPDP will serve as an independent regulatory authority with the power to conduct audits and inspections, and impose sanctions on companies or organizations that violate data protection regulations. The LPDP will also be responsible for handling regulatory violations, imposing sanctions, resolving disputes involving personal data breaches, and collaborating with law enforcement in more serious violation cases.

Meanwhile, the National Data Center (PDNS) focuses more on managing the national data infrastructure and providing secure data storage services for the government and public institutions.[29] The PDNS is responsible for ensuring that the data stored in the national data center are protected from cyber threats and can be accessed quickly and efficiently by government agencies. The PDNS does not have a mandate to oversee compliance with personal data protection regulations or to enforce laws related to personal data breaches. The primary function of the PDNS is to provide technology services and infrastructure, rather than oversight and law enforcement. The LPDP and PDNS have complementary roles but different focuses within the data protection and management ecosystem in Indonesia.

[29] Aptika Kominfo, 'Pusat Data Nasional – Ditjen Aptika', 2024, https://aptika.kominfo.go.id/tag/pusat-data-nasional/.

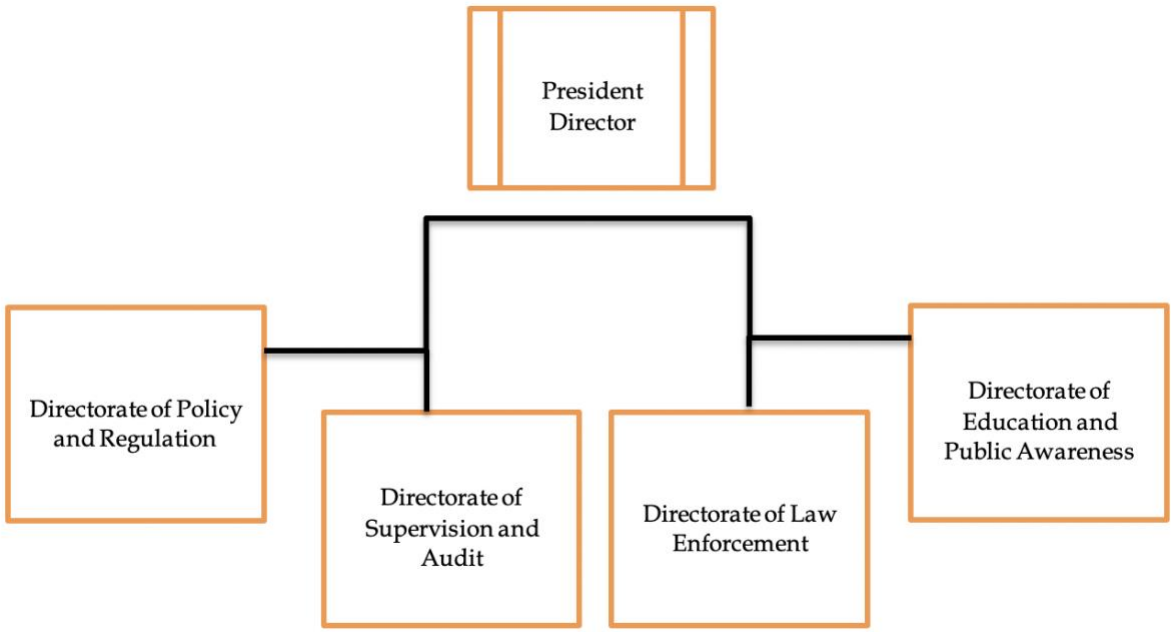

Figure 1 LPDP Structure Illustration

Figure 1 shows the proposed framework of The LPDP, consisting of several main directorates, including the Directorate of Policy and Regulation, the Directorate of Supervision and Audit, the Directorate of Law Enforcement, and the Directorate of Public Education and Awareness. Each Directorate has specific functions and responsibilities to ensure comprehensive and effective personal data protection.

1.3.1 Directorate of Policy and Regulation

This directorate is responsible for designing, developing, and updating the regulations relevant to personal data protection. The Directorate of Policy and Regulation must ensure that regulations align with international standards such as the General Data Protection Regulation (GDPR) in the European Union. The main functions of this directorate include policy analysis, stakeholder consultation, and drafting technical guidelines for regulatory implementation. In addition, the directorate must conduct ongoing research to identify new needs and challenges in personal data protection and formulate appropriate policy recommendations.

1.3.2 Directorate of Supervision and Audit

The Directorate of Supervision and Audit plays a key role in overseeing the compliance of companies and organizations with personal data protection regulations. This function includes conducting routine audits, surprise inspections,

and monitoring the implementation of data-protection measures. The directorate must be equipped with a team of experienced and trained auditors for cybersecurity and data protection. Furthermore, this directorate is responsible for developing and implementing reporting systems that allow the public and organizations to report data breaches or other violations.

1.3.3 Directorate of Law Enforcement

The Directorate of Law Enforcement is responsible for handling regulatory violations, imposing sanctions, and resolving disputes involving personal data breach. This includes the application of administrative fines and collaboration with law enforcement in more serious breach cases. The directorate must have a team of legal experts capable of assessing violations, determining appropriate sanctions, and pursuing legal processes, when necessary. Additionally, the directorate must have an effective dispute resolution mechanism, including mediation and arbitration, to help individuals and organizations resolve issues related to personal data protection.

The Directorate of Education and Public Awareness plays an equally important role in raising public awareness of their rights concerning personal data and how to protect them. This educational initiative includes public campaigns, training for companies, and provision of resources and guidance for individuals and organizations. According to research published by Bennett and Raab[30] public awareness and education are key components in the successful implementation of data protection policies. This directorate should develop comprehensive educational programs including seminars, workshops, and online educational materials accessible to the broader public.

1.3.4 Publik Directorate of Public Education and Awareness

The Directorate of Public Education and Awareness plays an equally important role in raising public awareness of their rights to personal data and how to protect it. This education includes public campaigns, training companies, and providing resources and guidelines for individuals and organizations. According to research published by Bennett and Raab, public awareness and education are key components in the successful implementation of data protection policies. This directorate must develop

[30] Bennett and Raab, *The Governance of Privacy*.

comprehensive educational programs including seminars, workshops, and online educational materials that are accessible to the general public.[31]

The implementation of effective personal data protection policies requires a structured, comprehensive approach. These policies must cover various aspects from establishing a strong regulatory framework to strict oversight to ensure compliance. One of the crucial first steps is to ensure that the independent Personal Data Protection Agency (LPDP) has authority and adequate resources to perform its duties. This agency must be responsible for issuing regulations, conducting audits, imposing sanctions, and providing operational guidance to companies and organizations that manage personal data. LPDP independence is crucial for avoiding political interference and ensuring that decisions are made in the interest of personal data protection rather than external pressures.

The Personal Data Protection Agency (LPDP) must ensure that the implemented regulations cover all the important aspects of personal data protection. This includes procedures for obtaining valid user consent, which must be explicit and well informed. Companies need to ensure that users understand how their data will be used, and give their consent voluntarily. Additionally, users must be given the right to withdraw their consent at any time, without negative consequences. These regulations should also establish obligations for companies to provide clear and easily understandable information regarding privacy policies and user rights.

Managing data access and deletion rights is another critical aspect of the policy implementation. Companies must have clear procedures for handling user data-access requests. Users should be able to know what data are collected, how they are used, and who has access to them. Furthermore, users should have the right to correct inaccurate data and delete data that are no longer required for legitimate purposes. The LPDP must ensure that companies implement adequate procedures to process these requests efficiently and in a timely manner.

Data security measures must also be a key focus in the implementation of regulations. Companies must apply appropriate technical and organizational measures to protect their personal data from unauthorized access, disclosure, or destruction. This includes encryption, firewalls, and strong authentication mechanisms. Moreover, companies should conduct regular risk assessments and update their security measures in accordance with the technological developments

[31] Bennett and Raab.

and cybersecurity threats. The LPDP must conduct periodic security audits to ensure that companies comply with established security standards.

The importance of education and training cannot be overlooked when implementing personal data-protection policies. The LPDP should develop a comprehensive public education program to raise awareness of people's rights to personal data. Public campaigns, workshops, and seminars should be conducted regularly to help people understand the importance of personal data protection and how to protect their own data. Additionally, companies should provide regular training to their employees on data protection policies and procedures. This training should cover both technical and non-technical aspects to ensure that all employees understand their role in protecting their personal data.

Supervision and law enforcement are key components of effective policy implementation. The LPDP must have the authority to conduct audits and surprise inspections of companies suspected of violating the regulations. This includes accessing company records, inspecting security systems, and interviewing staff members. If violations are found, the LPDP must be able to impose significant sanctions including hefty fines and other legal actions. Severe penalties provide strong incentives for companies to comply with regulations and take the necessary steps to protect personal data.

The lack of in-depth discussion on the Personal Data Protection Oversight Agency (LPDP) structure indicates that while the structure of the LPDP is described, it remains primarily descriptive and does not yet connect its establishment to the concept of an effective independent agency within public administration or administrative law theory. In public administration theory, an independent agency ideally has clear operational autonomy, allowing it to perform its oversight duties free from external interference, whether in political or business interests. This independence is essential for building public trust in the LPDP and ensuring consistent compliance with data-protection regulations. With this perspective in mind, the establishment of the LPDP in Indonesia should consider the principles of independence and effective governance to ensure that it functions in line with sound administrative principles.

Addressing potential challenges in coordinating LPDP with other agencies and possible conflicts of authority are also essential. As an agency responsible for oversight and enforcement in data protection, the LPDP needs to coordinate with various ministries and regulatory bodies, such as the Ministry of Communication and

Information Technology (Kominfo), the Financial Services Authority (OJK), and law enforcement agencies. Within administrative law theory, interagency coordination often presents challenges owing to differing objectives, procedures, and overlapping authorities. Without a well-defined framework to regulate these relationships, the LPDP may face obstacles in executing its role effectively. Developing detailed coordination regulations or guidelines could help reduce potential authority conflicts, enabling the LPDP to operate effectively within Indonesia's legal and administrative ecosystem.

Analysis of oversight and law enforcement remains underdeveloped. It is essential to explore how the concept of accountability should implement by the LPDP as an independent agency, specifically through mechanisms such as regular audits, administrative sanctions, and transparency obligations regulated by law. Establishing these measures would provide a clearer framework for the role of the LPDP in strengthening e-commerce companies' accountability in managing personal data. Regular audits would allow the LPDP to consistently assess compliance with data protection standards, whereas administrative sanctions would act as a deterrent against potential violations. Additionally, transparency obligations, such as the publication of compliance reports and findings, would ensure that both the LPDP and regulated companies are held publicly accountable. These mechanisms would create a structured approach to oversight that aligns with international standards, fostering a culture of accountability within Indonesia's e-commerce industry.

In addition, the LPDP must provide mechanisms for individuals to report personal data breaches and file complaints. These mechanisms must be easily accessible and efficient so that individuals feel safe and supported in reporting violations. The LPDP should also have a system in place to handle these complaints quickly and fairly, including providing compensation to individuals harmed by data breaches.

Collaboration between the LPDP and other government agencies, such as the Ministry of Communication and Informatics (Kominfo), is also important to ensure the coordinated implementation of policies. Kominfo can assist in drafting technical regulations and providing technological support for policy implementations. Cooperation with law enforcement is also essential to address serious violations and criminal activities.

Implementing an effective personal data protection policy requires a comprehensive and coordinated approach. The LPDP must have sufficient authority

and resources to carry out its duties, while companies must implement strict measures to protect personal data. Public education and employee training are also crucial to ensure that all parties understand the importance of personal data protection and know how to safeguard their data. Using a structured and comprehensive approach, Indonesia can ensure that its citizens' personal data are well protected in the digital age.

CONCLUSION

This study underscores the critical shortcomings of Indonesia's e-commerce ecosystem, particularly with regard to personal data protection. Despite regulatory frameworks, such as the ITE Law and PDP Law, enforcement and implementation mechanisms remain inadequate to address the dynamic challenges of e-commerce. Case studies, such as the 2020 Tokopedia data breach, reveal systemic vulnerabilities, including insufficient technical guidelines, weak enforcement of data protection measures, and a lack of clarity regarding the roles and responsibilities of entities managing user data. Furthermore, the absence of robust oversight mechanisms, such as an independent data protection agency, exacerbates the risks associated with data breaches, impacting user trust and overall security of the e-commerce landscape.

This study employs a comprehensive qualitative approach, leveraging the analysis of regulatory frameworks, case studies, and international comparisons to provide a nuanced understanding of personal data protection in Indonesia. This methodology enables an in-depth exploration of gaps in current policies and the potential role of an independent oversight body. By drawing parallels with international standards such as the GDPR, this study highlights actionable recommendations that align with global best practices while addressing Indonesia's specific needs. These findings contribute significantly to the discourse on digital governance and privacy in emerging economies, offering a roadmap for strengthening e-commerce security and compliance frameworks.

Although this study focuses on regulatory analysis and high-profile data breaches, it is inherently limited to exploring policy-level implications and selected case studies. This scope does not extend to an empirical examination of user behavior, business practices, or the economic costs of data breaches. However, these limitations provide opportunities for future research to include broader stakeholder perspectives and empirical data. Investigating the economic impact of data breaches, user attitudes toward privacy, and business compliance practices can provide a holistic view of personal data-protection challenges. Additionally, comparative studies of emerging

economies facing similar digitalization challenges can enrich the global understanding of adaptive and scalable data protection strategies.

DISCLOSURE

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

Funding Statement

No external funding was received for the study.

Authorship and Level of Contribution

The study was authored by Bilqis Laila Nuzul Sa'adah, Sukarmi, and Reka Dewantara, with each playing a significant role. Bilqis Laila Nuzul Sa'adah led the study's conceptualization, research objectives, theoretical framework, and initial manuscript drafting. Sukarmi focused on reviewing and analyzing regulatory frameworks, evaluating data protection standards, and refining discussions and conclusions. Reka Dewantara contributed to the literature review, data interpretation, and final manuscript editing to ensure academic rigor. All authors reviewed and approved the final version for submission and demonstrated a collaborative research effort.

Author Bionote

Bilqis Laila is a postgraduate law student at Universitas Brawijaya, Indonesia. Her research focuses on business law and she is actively pursuing academic growth in the field of law through her studies and research projects. Sukarmi is a professor of law and lecturer at the Universitas Brawijaya, Indonesia. With extensive experience in legal studies, she has published widely and contributed significantly to business law, shaping the development of legal education in Indonesia. Reka Dewantara is a law lecturer at Universitas Brawijaya, Indonesia. Her teaching and research focus on business law and she has been involved in various academic publications, contributing to the advancement of legal knowledge at the university.

BIBLIOGRAPHY

Abdurrohim, Muhammad, Indah Kumalasari, and Fathur Rosy. 'The Paradox of Indonesia Cyberspace Policy and Cooperation: Neoclassical Realism Perspective'. *Jurnal Hubungan Internasional* 11, no. 2 (19 September 2022): 13–23. https://doi.org/10.18196/jhi.v11i2.14361.

Aji, Muhammad Prakoso. 'Sistem Keamanan Siber Dan Kedaulatan Data Di Indonesia Dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]'. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional* 13, no. 2 (4 January 2023): 222–38. https://doi.org/10.22212/jp.v13i2.3299.

Aldiyansyah, Muhamad Nur, Fatya Alty Amalia, and Gundur Leo. 'Understanding the Effect of E-Commerce Security Towards Loyalty': Bandung, Indonesia, 2021. https://doi.org/10.2991/aer.k.211106.093.

APJII. 'Kasus Data Pribadi Yang Selalu Bocor'. Jakarta: Asosiasi Penyelenggara Jasa Internet Indonesia, 2021. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://apjii.or.id/assets/media/buletin_apjii_edisi_94_-_september_2021_bulletin.pdf.

Aptika Kominfo. 'Pusat Data Nasional – Ditjen Aptika', 2024. https://aptika.kominfo.go.id/tag/pusat-data-nasional/.

Bennett, Colin J., and Charles D. Raab. *The Governance of Privacy: Policy Instruments in Global Perspective*. 1st ed. Routledge, 2017. https://doi.org/10.4324/9781315199269.

Chassang, Gauthier. 'The Impact of the EU General Data Protection Regulation on Scientific Research'. *Ecancermedicalscience* 11 (3 January 2017). https://doi.org/10.3332/ecancer.2017.709.

CNBC. 'Hackers Raid eBay in Historic Breach, Access 145M Records', 2014. https://www.cnbc.com/2014/05/22/hackers-raid-ebay-in-historic-breach-access-145-mln-records.html.

CNN Indonesia. 'Kronologi Lengkap 91 Juta Akun Tokopedia Bocor Dan Dijual', 2020. https://www.cnnindonesia.com/teknologi/20200503153210-185-499553/kronologi-lengkap-91-juta-akun-tokopedia-bocor-dan-dijual.

Derindağ, Ömer Faruk. 'Rise of Cross-Border E-Commerce: A Systematic Literature Review'. *Journal of Applied And Theoretical Social Sciences* 4, no. 3 (11 September 2022): 352–72. https://doi.org/10.37241/jatss.2022.71.

Dinev, Tamara, Heng Xu, Jeff H Smith, and Paul Hart. 'Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts'. *European Journal of Information Systems* 22, no. 3 (May 2013): 295–316. https://doi.org/10.1057/ejis.2012.23.

Ensign Infosecurity. 'Cyber Threat Landscape Report 2024'. Accessed 31 July 2024. https://www.ensigninfosecurity.com/resources/threat-insights/cyber-threat-landscape-report-2024?utm_source=google&utm_medium=cpc&utm_campaign=cti_report_2024&gad_source=1&gclid=Cj0KCQjwwae1BhC_ARIsAK4Jfrzrw_y4mvCoLNXpkwMqDmLX6KKDasvKBgUvIqjvpBv0IOcOl4oAslUaAuxTEALw_wcB.

Fung, Archon, Mary Graham, and David Weil. *Full Disclosure: The Perils and Promise of Transparency*. Inggris: Cambridge University Press, 2007.

Goddard, Michelle. 'The EU General Data Protection Regulation (GDPR): European Regulation That Has a Global Impact'. *International Journal of Market Research* 59, no. 6 (November 2017): 703–5. https://doi.org/10.2501/IJMR-2017-050.

IBM Security. 'Cost of a Data Breach 2024 | IBM', 2020. https://www.ibm.com/reports/data-breach.

Javelin. 'Identity Fraud Study | Javelin', 2021. https://www.javelinstrategy.com/annual-identity-fraud-study.

P. Romansky, Radi, Irina S. Noninska, 1 Department of Informatics, Technical University of Sofia, Sofia 1000, Bulgaria, and 2 Department of Computer Systems, Technical University of Sofia, Sofia 1000, Bulgaria. 'Challenges of the Digital Age for Privacy and Personal Data Protection'. *Mathematical Biosciences and Engineering* 17, no. 5 (2020): 5288–5303. https://doi.org/10.3934/mbe.2020286.

Privacy Rights. 'Data Breach Chronology | Privacy Rights Clearinghouse', 2020. https://privacyrights.org/data-breaches.

Rahayu, Rita, and John Day. 'E-Commerce Adoption by SMEs in Developing Countries: Evidence from Indonesia'. *Eurasian Business Review* 7, no. 1 (April 2017): 25–41. https://doi.org/10.1007/s40821-016-0044-6.

Salim, Samuel Christian, and Jeane Neltje. 'Analysis of Legal Protection Towards Personal Data in E-Commerce': Jakarta, Indonesia, 2022. https://doi.org/10.2991/assehr.k.220404.101.

Shabani, Mahsa, and Pascal Borry. 'Rules for Processing Genetic Data for Research Purposes in View of the New EU General Data Protection Regulation'. *European Journal of Human Genetics* 26, no. 2 (February 2018): 149–56. https://doi.org/10.1038/s41431-017-0045-7.

Thales Group. 'Lack of Consumer Trust across Industries to Protect Their Personal Data, New Research from Thales Has Revealed | Thales Group', 2021. https://www.thalesgroup.com/en/countries-europe/romania/press_release/lack-consumer-trust-across-industries-protect-their-personal.

Tikkinen-Piri, Christina, Anna Rohunen, and Jouni Markkula. 'EU General Data Protection Regulation: Changes and Implications for Personal Data Collecting Companies'. *Computer Law & Security Review* 34, no. 1 (February 2018): 134–53. https://doi.org/10.1016/j.clsr.2017.05.015.

Ventures and Cybersecurity. 'Cybersecurity Jobs Report'. Herjavec Group 1, 2017.

Westin, Alan F. 'Social and Political Dimensions of Privacy'. *Journal of Social Issues* 59, no. 2 (July 2003): 431–53. https://doi.org/10.1111/1540-4560.00072.

You, Ilsun, Marek R. Ogiela, Isaac Woungang, and Kangbin Yim. 'Innovative Security Technologies against Insider Threats and Data Leakage'. *International Journal of Computer Mathematics* 93, no. 2 (February 2016): 236–38. https://doi.org/10.1080/00207160.2015.1044784.

Zuboff and Shoshana. *The Age of Surveillance Capitalism Social Theory Re-Wired.* England: Routledge, 2023.