


Legal Protection Of Consumers Against Misuse Of Personal Data By Business Actors In The Digital Era

Yuniar Rahmatiar

Universitas Buana Perjuangan, Karawang, Indonesia

Article Info	ABSTRACT
<p>Keywords: Consumer protection, personal data, digital era, regulation, data misuse.</p>	<p>Amidst the rapid development of information technology, consumer personal data has become a very valuable asset for business actors, but this also increases the risk of misuse. This study aims to analyze various forms of Consumer Legal Protection against Misuse of Personal Data by Business Actors in the Digital Era. The research method used is normative juridical with a legislative approach and case studies. The research results show that the misuse of personal data by business actors in the digital era poses serious risks to consumers, including unauthorized data collection, fraud, and discrimination, which can damage the trust and reputation of the company. The losses from this abuse are not only financial, but also emotional and reputational, impacting individuals' mental health and their access to financial services. In Indonesia, consumer legal protection against personal data abuse is regulated in the 1945 Constitution of the Republic of Indonesia and Law Number 27 of 2022 concerning Personal Data Protection, which affirms the individual's right to feel safe. Controllers and processors of personal data are responsible for maintaining the confidentiality and integrity of data, while the appointment of a competent data protection officer is essential to ensure compliance with regulations and minimize violations. Through these steps, it is hoped that personal data protection can be implemented effectively, creating a safe digital environment and increasing consumer trust .</p>
<p>This is an open access article under the CC BY-NC license</p> 	<p>Corresponding Author: Yuniar Rahmatiar Universitas Buana Perjuangan, Karawang, Indonesia yuniar@ubpkarawang.ac.id</p>

INTRODUCTION

The development of information and communication technology (ICT) has significantly changed the way information and data are distributed throughout the world. This technology allows information to be distributed quickly, widely, and efficiently without geographical limitations (Nugroho, 2016). Advances in internet networks, software and hardware allow data to be exchanged in seconds, which used to take much longer with traditional media. This development brings great benefits in terms of global accessibility and connectivity, but also raises new challenges related to data security and privacy (Pakarti et al., 2023). This transformation drives the need for stricter regulations to manage the distribution of information safely and responsibly in this digital era.

Digital transactions conducted online and quickly have encouraged instant exchange of information in various sectors, from e-commerce to financial services. Every time

consumers interact with a digital platform—whether to make a purchase, subscribe to a service, or simply browse—data about their behavior, preferences, and activities is automatically collected (Akhmaddhian & Agustiwi, 2016). This transaction process not only involves identity data but also includes sensitive information such as transaction history, location, and device used. In seconds, this data is processed to meet consumer needs efficiently (Kesuma et al., 2021). However, behind the speed and convenience offered, this phenomenon also contributes to the formation of very large and complex data volumes, which we know as big data (Khotimah & Chairunnisa, 2016).

Big data, the result of the accumulation of large amounts of data from digital transactions, has strategic value for business actors because it can be analyzed to identify consumer behavior patterns, market preferences, and predict future trends (Ranto, 2019). Through big data analysis, companies can make more informed business decisions, improve service personalization, and design more effective marketing strategies. However, along with these potential benefits, big data management also brings its own challenges, especially related to consumer data privacy and security (Benuf et al., 2019).

Currently, misuse of personal data by business actors is increasingly common, and this raises significant concerns among the public. Many companies, both large and small, collect personal data without explicit permission from the data owner, and use the information for non-transparent purposes, such as aggressive marketing, selling data to third parties, or even fraud (Aryani & Susanti, 2022). Cases of data leaks that result in sensitive information, such as identity numbers, financial information, and other personal data, falling into the wrong hands, further exacerbate the situation. This phenomenon not only damages consumer trust in business actors but also has long-term detrimental impacts on individuals who become victims, including the risk of identity theft and financial loss (Poernomo, 2023).

To protect people's personal data in the digital era, the government has taken an important step by issuing Law Number 27 of 2022 concerning Protection of Personal Data. This law is the legal basis for regulating the collection, use, and protection of personal data carried out by various parties, including individuals and business entities (Fauzy et al., 2022). As digital activities, such as online transactions and the use of social media, become increasingly widespread, personal data becomes vulnerable to misuse. This law seeks to ensure that all personal data processed is protected with adequate security standards and that people's rights to their data privacy are respected (Yudistira & Ramadani, 2023).

One of the main provisions in this law is that every individual, including those running a small business or e-commerce from home, can be categorized as a personal data controller (Priliasari, 2023). As data controllers, they are legally responsible for the processing of personal data carried out, such as obtaining consent from the data owner, maintaining confidentiality, and using the data only for legitimate purposes permitted by law. This responsibility applies to all business actors, regardless of the scale of their business, thus ensuring that personal data protection is applied widely and consistently (Kosegeran, 2022).

In addition, this law emphasizes the importance of transparency in the management of personal data. Data controllers are required to provide clear explanations to data owners

regarding the purpose of data collection, how the data will be processed, and who will have access to it (Sulistianingsih et al., 2023). Data owners also have the right to access, correct, or request deletion of their data if necessary. Thus, this law not only provides protection against data misuse, but also empowers the public to control their personal information, as well as encourages the creation of a safer and more trustworthy digital environment (Manurung & Thalib, 2022).

The concept and provisions regarding personal data protection are not new to the financial services sector, especially banking. Even before the enactment of Law Number 27 of 2022 concerning Personal Data Protection, this sector was already regulated by various regulations aimed at protecting the privacy and security of consumer data (Nababan & Lasmadi, 2023). The Financial Services Authority has issued Financial Services Authority Regulation Number 6/POJK.07/2022 which emphasizes the importance of obtaining consumer consent before business actors collect, use, and store their personal data (Najla et al., 2023). This regulation provides a clear legal basis for banks and other financial institutions to ensure that consumer data is processed ethically and in accordance with the consent given by the consumer. Through this Financial Services Authority Regulation, business actors are required to be transparent in the use of personal data, provide clear information about the purpose of using the data, and protect data from unauthorized access (Anisa & Syahrin, 2023).

The regulations implemented by the Financial Services Authority are in line with the principles in the Personal Data Protection Law which was enacted later, and complement consumer protection efforts in the financial services sector (Rahman, 2021). This provision not only creates an obligation for financial institutions to protect personal data, but also gives consumers greater control over their information. Consumers have the right to know how their data is used, as well as the right to refuse the use of their data outside of the consent that has been given (Saly & Sulthanah, 2023). These steps strengthen consumers' sense of security in transacting in the digital world, where personal data is a very valuable asset. With the synergy between the Financial Services Authority Regulation and the Personal Data Protection Law, the financial sector in Indonesia can be better prepared to face data security challenges and maintain consumer trust in the increasingly complex digital era (Tektona & Roziqin, 2020).

The purpose of this research on consumer legal protection against misuse of personal data by business actors in the digital era is to identify various forms of misuse of personal data that occur, analyze their impact on consumers, and evaluate the effectiveness of protection policies that have been implemented by the government and related institutions. The benefits of this research are to increase public awareness of their rights related to personal data, provide useful information for business actors in implementing ethical and regulatory data management practices, and encourage the government to strengthen regulations and law enforcement mechanisms against misuse of personal data, so as to create a safer and more trustworthy digital environment for all parties.

METHOD

This research was conducted using a normative legal approach, which focuses on data collection through literature studies. The data sources used include laws, official documents, books, magazines, and other literature relevant to the research topic (Soekanto, 2007). The main focus of this research is to examine the provisions of positive law applicable in Indonesia related to the legal protection of consumer personal data from misuse by business actors in the financial financing and services sector. To achieve this goal, the problem-solving methods applied include the statute approach, which examines various existing regulations, and the conceptual approach (Ariawan, 2013), which seeks to examine the theories and concepts underlying personal data protection. In this way, this research is expected to provide a comprehensive picture of the legal framework that protects consumers and the challenges faced in its implementation in the digital era.

RESULT AND DISCUSSION

Forms of Misuse of Personal Data by Business Actors in the Digital Era

Consumer personal data protection is increasingly becoming a major concern amidst the rapid growth of internet and social media usage. Personal information, such as names, addresses, telephone numbers, and other data collected by various platforms and service providers, has become a valuable asset for many parties (Silalahi & Dameria, 2023). Although this data collection is often carried out for legitimate business purposes, such as marketing and improving services, there are significant potential risks that need to be watched out for, including the possibility of data misuse. There are several forms of misuse of personal data by business actors in the digital era:

1. Unauthorized Data Collection

Many businesses today collect consumers' personal data without their explicit consent, often through the use of cookies on websites or apps. Cookies are small files stored on a user's device that allow a website to remember certain information about them, such as preferences or browsing history. While cookies can improve the user experience by providing more relevant content, many companies are not transparent about how and for what purposes the data collected will be used. In many cases, users are not given enough information to make informed decisions about the collection and use of their data, creating a potential privacy breach.

This practice of collecting data without consent is not only detrimental to consumers, but can also cause legal problems for business actors. With increasing public awareness of the importance of data privacy and consumer protection, a number of countries have begun to implement strict regulations regarding the collection and use of personal data. The Personal Data Protection Act in Indonesia, for example, requires businesses to obtain explicit consent from consumers before collecting and using their personal data. Therefore, it is important for businesses to not only comply with existing regulations but also build trust with consumers through transparent and ethical data management practices. This will create a better relationship between companies and consumers, as well as increase customer loyalty in the long run.

2. Misuse of Data for Marketing

Personal data collected by businesses is often used for aggressive marketing purposes, which can result in a less than pleasant user experience. By leveraging information such as browsing history, product preferences, and demographics, companies can build highly detailed consumer profiles. This allows them to target ads to individuals in a more precise manner. However, this marketing strategy is not always well received by consumers, as they often receive irrelevant or unsolicited ads. When these ads appear continuously, consumers can feel annoyed, even feeling that their privacy is being violated, which can ultimately damage the company's image and cause consumers to switch to competitors who respect their privacy more.

In addition, sending these irrelevant ads can have negative implications for the relationship between companies and consumers. Many consumers feel that they have no control over the personal information they share and how it is used. This dissatisfaction can result in decreased trust in the brand and reduce customer loyalty. For this reason, it is important for business actors to re-evaluate their marketing strategies and ensure that the approaches used are not only effective, but also ethical and respect consumer privacy rights. Implementing transparent policies and giving consumers the option to control how their data is used can help companies build stronger, more positive relationships with their customers, while improving their brand reputation in the marketplace.

3. Sales of Data to Third Parties

Some businesses engage in harmful practices by selling consumers' personal data to third parties, such as marketing companies or data brokers, without the knowledge or consent of the individuals concerned. This sold data often includes sensitive information, such as purchase history, consumer preferences, and demographic information that can be used to more aggressively target ads. This practice not only violates consumers' privacy rights, but also raises concerns about how the data will be used once it is sold. Consumers, who may not be aware that their data is being traded, are potentially targeted for more intensive and sometimes misleading marketing campaigns, which can harm their overall user experience.

The consequences of selling personal data are not only limited to privacy violations, but can also cause wider harm to consumers. In some cases, the data that has been sold may be used for harmful purposes, such as fraud or identity theft. When personal information falls into the wrong hands, individuals can face serious consequences, including financial loss and negative impacts on their reputation. To address this issue, more and more countries are starting to introduce strict regulations regarding the collection, use and sale of personal data. Companies are expected to be more responsible and transparent in managing consumer data, and provide individuals with greater control over the information they share, thereby creating a safer digital environment and protecting consumer rights.

4. Data Leak

Security breaches resulting in data leaks are one of the most critical issues in today's digital era. When sensitive consumer information, such as identity numbers, financial information, or email addresses, falls into the wrong hands, the impact can be devastating.

These leaks often occur due to cyber attacks, such as hacking, malware, or even internal negligence in companies that do not have adequate security systems. In many cases, companies are not aware that their data has been compromised until after the incident occurs, further exacerbating the situation. When such personal data is stolen, individuals are at risk of identity theft, financial fraud, and other forms of abuse that can disrupt their daily lives.

In addition to the direct impact on individuals, data breaches also have broader consequences for companies and the industry as a whole. The reputation of the company involved can be significantly damaged, reducing consumer trust and causing a decrease in revenue. Many consumers will think twice before sharing their personal data with a company that has experienced a data breach, which in turn can hinder business growth. Therefore, it is important for businesses to implement strong security measures to protect consumer data, including using encryption, intrusion detection systems, and training employees on security best practices. By doing this, companies not only protect consumers but also maintain their reputation and business sustainability in an increasingly competitive market.

5. Phishing and Fraud

The use of personal data that has been collected to commit fraud is one of the most detrimental practices that occurs in the digital world today. One common method of fraud is to create a fake website that looks like the official website of a company or institution. Fraudsters use the personal information they have collected, such as names, addresses, and financial information, to design the site to look legitimate and convincing. In this way, they try to attract the attention of unsuspecting consumers and encourage them to fill in sensitive information, such as credit card numbers or passwords. When consumers are fooled into entering their data, the fraudsters can then use the information for personal gain, such as stealing money, accessing accounts, or even selling the information to third parties for malicious purposes.

These types of fraudulent practices not only harm individuals, but can also cause significant harm to brands whose sites are being spoofed. When consumers learn that they have been victims of fraud, their trust in the genuine company or brand can plummet, potentially even damaging the company's reputation as a whole. This can result in significant loss of customers and revenue. Therefore, it is important for businesses to raise consumer awareness of the signs of fraud and provide education on how to protect their personal information. In addition, businesses should invest in advanced security technologies and implement best practices to protect consumer data, as well as maintain transparency in data management, to build trust and security in an increasingly complex digital environment.

6. Use of Data for Discrimination

The use of personal data to discriminate against consumers is becoming an increasingly prominent issue as technology advances and data collection expands. In this practice, businesses can implement different pricing strategies based on certain consumer profiles or behaviors, known as price discrimination. For example, a consumer who

frequently shops online may be charged a higher price for a particular product compared to another consumer who is less active in shopping. Using algorithms that analyze data from purchase history, location, and even online searches, companies can adjust prices in a way that is detrimental to certain groups of consumers. This practice not only creates an unfair shopping experience, but can also lead to dissatisfaction and loss of trust among customers.

In addition to the impact on consumers, the use of data to discriminate can also have negative implications for a company's image and reputation. When consumers realize that they are being treated unfairly based on their profiles, this can trigger negative reactions, such as public outcry and decreased brand loyalty. In some cases, such actions may attract the attention of regulators, who may consider new policies or laws to protect consumers from these discriminatory practices. Therefore, it is important for companies to implement fair and transparent policies in managing consumer personal data, and ensure that all customers are treated fairly regardless of their background or behavior. In this way, companies not only protect consumers but also build a positive reputation that can increase competitiveness in the market.

The Impact of Misuse of Personal Data by Business Actors on Consumers

Personal data leaks are a problem that requires serious attention from all parties, including individuals, companies and governments. In today's digital era, where information can be easily accessed and shared, the risk of data leaks is increasing, which can threaten individual privacy and security. When sensitive data, such as identity numbers, financial information, or health history, falls into the wrong hands, the consequences can be devastating, ranging from identity theft to financial fraud for consumers. The following are a number of impacts of misuse of personal data by business actors on consumers.

1. Financial Fraud

When consumers fall victim to financial fraud due to the leakage of sensitive information such as bank account numbers or credit card information, the impact can be devastating. Fraudsters who gain access to this data can then make unauthorized transactions, withdraw funds, or purchase goods and services without the account holder's knowledge. In many cases, these frauds occur quickly and undetected, so consumers often only realize they have been victimized after the loss has already occurred. Not only does this result in immediate financial loss, it can also add to the financial burden, especially if the consumer does not have sufficient reserves to cover the loss.

The process of recovering from financial fraud is often complex and time-consuming. Consumers who lose money should contact their bank or financial institution to report the fraud and block access to their account. However, recovery of funds is not always guaranteed, and some institutions may take a long time to investigate the case before returning lost funds. During this time, consumers may feel unsafe and stressed, potentially jeopardizing their financial stability. Additionally, these experiences can discourage consumers from using digital financial services in the future, hindering progress in wider adoption of financial technology. Therefore, it is important for consumers to remain vigilant and take proactive steps to protect their personal information from potential misuse.

2. Privacy Intrusion

Misuse of personal data can have a significant impact on consumer privacy, creating feelings of discomfort and surveillance. When individuals become aware that their personal information is being used without their permission or for purposes they did not agree to, they may feel like objects that are being continuously monitored and analyzed. For example, excessive data collection by social media platforms or online services can make consumers feel that their every move on the internet is being recorded and evaluated, which in turn creates a sense of loss of control over their personal information. This data openness not only impacts individual comfort, but can also cause anxiety about how the data can be used, accessed, or even misused by third parties.

This situation can lead to erosion of consumer trust in the companies and services they use. When consumers feel that their privacy is not being respected, they tend to withdraw from interacting with that company, either by reducing their use of the service or by considering switching to a more privacy-respecting alternative. This loss of trust not only impacts a company's relationship with customers, but can also impact the brand's reputation in the wider market. Companies that fail to protect consumers' personal data and are not transparent about how they use it risk public criticism, reduced customer loyalty, and even potential financial losses. Therefore, it is essential for companies to implement strict data protection policies and commit to safeguarding consumer privacy in order to rebuild and maintain the trust that is vital to business relationships .

3. Stress and Anxiety

Learning that their personal data has been misused can cause deep stress and anxiety for consumers. When individuals realize that their sensitive information, such as their name , address, or financial information, has been accessed by unauthorized parties, their sense of security is shaken. This feeling can develop into a greater fear of further potential misuse, such as identity theft or fraud. Every time they receive a suspicious advertising offer or experience a disruption in their online accounts, this anxiety can increase, creating a recurring cycle of stress related to privacy and data security.

In addition to the emotional impact, uncertainty about the use of personal data can also impact consumers' mental health and overall well-being. Prolonged stress can contribute to other mental health problems, such as anxiety and depression. Consumers may feel trapped in uncertainty, constantly thinking about the possible consequences of their data being misused. This can result in a decreased quality of life, as the individual may avoid social interactions or digital transactions that may exacerbate feelings of threat. In the long term, these impacts will not only affect individuals, but also society as a whole, as they increase the burden on mental health and social systems. Therefore, it is imperative for companies and governments to take stricter and more transparent protection measures in the management of personal data to ease concerns and restore public trust .

4. Reputational Loss

When a consumer's personal information is misused to spread inaccurate or damaging information, the impact can be devastating, especially to the individual's reputation. For example, if the data is used to spread rumors or slander on social media, the

targeted individual can suffer significant damage to their reputation . This false information can spread quickly in the digital age, resulting in a loss of credibility with friends, family, and coworkers. In some cases, this can have a direct impact on their career and professional opportunities, such as losing a job, difficulty getting a promotion, or even losing clients if they are a professional or entrepreneur.

Furthermore, reputational damage caused by the spread of misinformation can affect an individual's social and professional relationships. When others begin to doubt a person's integrity or honesty due to false information, hard-earned relationships can be destroyed in a short time. The individual may feel isolated and lose social support, which in turn can worsen their mental health. The loss of these positive social networks not only disrupts emotional well-being, but can also impact an individual's ability to thrive in their career and personal life. Therefore, it is important to implement better protection mechanisms for personal data, so that consumers can avoid the risk of misuse of information that can damage their reputation and relationships.

5. Difficulty in Obtaining Service

Consumers who are victims of personal data misuse often face significant challenges in accessing financial services or credit in the future. When their personal information is used to commit fraud, such as opening a credit account without permission, it can create a negative record in the credit reporting system. Creditors and financial institutions typically rely on credit reports to assess an applicant's eligibility for a loan or financial facility. With a negative record, consumers can be considered high risk, so they are potentially rejected when applying for credit or even charged a higher interest rate. The inability to obtain credit can limit their access to a range of important financial services, including loans for education, home purchases, or business capital.

Furthermore, the impact of this data misuse can be long-term, making it difficult to rebuild a good credit reputation. Consumers may need to spend time and resources to repair their credit history, which can involve a lengthy process of contesting errors on their credit report or working with financial institutions to regain their trust. During this time, individuals may feel trapped in a financially disadvantaged situation, making them more vulnerable to stress and distress. Uncertainty about their financial future can reduce their confidence and prevent them from taking proactive steps to plan for the future, such as investing in education or starting a new business. Therefore, it is important for consumers to have better protections against personal data misuse, so that they can have fair and equal access to financial services.

6. Losing Trust

Misuse of personal data can lead to a breakdown in consumer trust in businesses and entire industries. When consumers witness or hear about cases of data misuse, they tend to become skeptical of companies' intentions and practices in managing personal information. This sense of insecurity can make them think twice before interacting with digital platforms, especially those that ask for sensitive information. As a result, this distrust can hinder growth and innovation in the digital sector, as many consumers hold back from taking advantage of the convenience and benefits that modern technology offers. In the long term,

this decline in trust not only hurts consumers, but can also negatively impact the reputation and sustainability of businesses committed to ethical practices and data protection.

Furthermore, this loss of trust can reduce consumer engagement in digital transactions, which can impact business profitability. If consumers are reluctant to share personal information or make online purchases, then the potential revenue for businesses will decrease. This can cause businesses to lose loyal customers and face difficulties in attracting new ones, especially in an era where seamless digital experiences are key to winning over consumers. With the uncertainty around data security, businesses may find themselves trapped in a cycle of declining trust and revenue, ultimately affecting their competitiveness in the market. Therefore, businesses must proactively implement strong and transparent data protection measures to restore consumer trust and ensure the sustainability of their businesses in this digital era.

Legal Protection of Consumers against Misuse of Personal Data by Business Actors

Indonesia guarantees protection of personal data for its citizens through provisions in the constitution, specifically in Article 28G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia. This provision affirms the right of every individual to receive protection for himself, his family, his honor, his dignity, and the property under his control. With this article, the state recognizes that everyone has the right to feel safe and protected from various threats, including the potential misuse of personal data that can harm their personal and social lives. This shows the state's commitment to respecting and protecting human rights, especially in the context of increasingly rapid developments in information technology.

Furthermore, this provision provides a strong legal basis for personal data protection efforts in Indonesia. By making the right to personal data protection a part of human rights, the state is obliged to create regulations and policies that support the implementation of this protection. This becomes increasingly important in the digital age, where the collection and use of personal data often occurs without the individual's knowledge or consent. Therefore, strengthening personal data protection must be balanced with public education about their rights and the steps that can be taken to protect their personal information. Thus, not only the state is responsible, but also individuals need to be aware of the importance of maintaining and protecting their personal data in an increasingly complex digital environment.

The Personal Data Protection Law in Indonesia is a real implementation of the provisions contained in Article 28G Paragraph (1) of the 1945 Constitution of the Republic of Indonesia. This law regulates the roles and responsibilities of personal data controllers and personal data processors. Personal data controllers are defined as individuals, public bodies or international organizations that act either individually or collectively in determining the purposes and controlling the processing of personal data. These personal data controllers have significant authority to determine how personal data is processed and used, and they must carry out these responsibilities with integrity and transparency.

Meanwhile, personal data processors are entities that process personal data on behalf of personal data controllers. This includes individuals, public bodies, or international

organizations involved in data processing activities. The personal data processor does not have the right to determine the purposes of data processing, but must carry out the instructions of the personal data controller. Therefore, the relationship between the controller and the processor of personal data is critical to ensure that personal data is managed in accordance with applicable regulations and the rights of personal data subjects are properly protected.

In the context of responsibilities, the Personal Data Protection Law regulates various obligations for personal data controllers in Articles 20 to 50. Some of these obligations include showing proof of consent given by the personal data subject before processing, maintaining the confidentiality of personal data, and preventing unauthorized access to personal data. This emphasizes the importance of transparency and accountability in the management of personal data, so that data subjects feel safe and protected.

On the other hand, personal data processors have obligations as stipulated in Articles 51 to 52. Among these obligations are processing personal data based on instructions from the personal data controller, as well as obtaining written consent from the personal data controller before involving third parties in data processing. With these provisions, the Personal Data Protection Law not only provides a clear legal framework, but also emphasizes the importance of secure and trusted collaboration between data controllers and processors in maintaining the integrity of personal data.

Personal data controllers and personal data processors have an obligation to appoint officials or officers who are responsible for carrying out personal data protection functions. The appointment of these officials or officers must be based on professionalism, knowledge of applicable laws, personal data protection practices, and adequate ability to carry out the mandated tasks. This demonstrates the commitment of personal data controllers and processors to maintain data integrity and effectively protect the rights of personal data subjects.

The main duties of officials or officers who carry out personal data protection functions include several important aspects. First, they are responsible for informing and advising personal data controllers or personal data processors so that they can comply with the provisions set out in the Personal Data Protection Act. This task is critical to ensure that all parties involved in the processing of personal data understand their legal obligations and implement best practices in data management.

In addition, the personal data protection officer or officer also has the responsibility to monitor and ensure compliance with the Personal Data Protection Act and the policies set by the personal data controller or personal data processor. By actively monitoring, they can detect potential breaches or deficiencies in existing data protection practices. This action is expected to minimize the risk of misuse of personal data and create a safer environment for data subjects.

In addition, the official or officer must provide advice on the assessment of the impact of personal data protection. They need to monitor the performance of personal data controllers and processors in implementing effective data protection practices. Lastly, this official or officer also acts as a coordinator and contact person for issues related to the

processing of personal data. Through this role, they can ensure good communication between the various parties involved, as well as ensure that all issues related to personal data protection are addressed seriously and in a timely manner. Thus, the role of personal data protection officers or officers is key in creating trust and security in the processing of personal data.

CONCLUSION

Misuse of personal data by businesses in the digital era creates various serious risks for consumers, including unauthorized data collection, misuse for marketing, selling data to third parties, data leaks, fraud, and discrimination. While data collection is often done for legitimate business purposes, these practices can damage consumer trust and negatively impact a company's reputation. In facing these challenges, it is important for businesses to implement strict regulations, implement transparent and ethical data management practices, and raise consumer awareness of the risks involved. In this way, companies can create a safer digital environment, protect consumer rights, and build stronger, more sustainable relationships with customers.

Misuse of personal data by businesses has serious consequences for consumers, including financial, emotional and reputational harm. Financial fraud can result in immediate losses and disrupt an individual's financial stability, requiring a long time to recover. Additionally, privacy intrusions reduce consumers' sense of security and control over their personal information, potentially eroding trust in companies and damaging their reputations. The stress and anxiety that arises from data misuse can impact individuals' mental health and quality of life, as well as create a burden on public health systems. Reputational losses resulting from the spread of false information can damage careers and social relationships, while difficulties in obtaining financial services limit consumers' access to essential products and impair their ability to build a good credit reputation. In addition, loss of trust in business actors and the industry as a whole can hamper growth and innovation in the digital sector, as well as negatively impact company profitability.

Consumer legal protection against misuse of personal data in Indonesia is regulated in the 1945 Constitution of the Republic of Indonesia and is further elaborated in Law Number 27 of 2022 concerning Protection of Personal Data. This provision affirms the right of individuals to feel safe and protected from potential misuse of personal data, while also requiring the state to create regulations that support such protection. Controllers and processors of personal data have a responsibility to maintain the integrity and confidentiality of data, and to carry out transparency and accountability obligations. The appointment of a competent data protection officer is crucial in ensuring compliance with regulations, monitoring data protection practices and providing necessary advice to prevent breaches. With these steps, it is hoped that personal data protection can be realized effectively, providing a sense of security for consumers and supporting trust in an increasingly complex digital ecosystem.

REFERENCES

1. Akhmaddhian, S., & Agustiwati, A. (2016). Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Jual Beli Secara Elektronik Di Indonesia. *UNIFIKASI: Jurnal Ilmu Hukum*, 3(2), 40-60.
2. Anisa, Y., & Syahrin, M. A. (2023). Pelaksanaan Peraturan Ojk Ri No. 6/Pojk. 07/2022 Tentang Perlindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan Online Di Kota Pekanbaru. *Journal of Sharia and Law*, 2(1), 312-334.
3. Ariawan, I. G. K. (2013). Metode Penelitian Hukum Normatif. *Kertha Widya*, 1(1).
4. Aryani, A. P., & Susanti, L. E. (2022). Pentingnya perlindungan data pribadi konsumen dalam transaksi online pada marketplace terhadap kepuasan konsumen. *Ahmad Dahlan Legal Perspective*, 2(1), 20-29.
5. Benuf, K., Mahmudah, S., & Priyono, E. A. (2019). Perlindungan Hukum Terhadap Keamanan Data Konsumen Financial Technology Di Indonesia: Indonesia. *Refleksi Hukum: Jurnal Ilmu Hukum*, 3(2), 145-160.
6. Fauzy, E., & Shandy, N. A. R. (2022). Hak Atas Privasi dan Politik Hukum Undang-Undang Nomor 27 Tahun 2022 Tentang Pelindungan Data Pribadi. *Lex Renaissance*, 7(3), 445-461.
7. Kesuma, A. N. D. H., Budiarta, I. N. P., & Wesna, P. A. S. (2021). Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial Dalam Transaksi Elektronik. *Jurnal Preferensi Hukum*, 2(2), 411-416.
8. Khotimah, C. A., & Chairunnisa, J. C. (2016). Perlindungan hukum bagi konsumen dalam transaksi jual beli-online (e-commerce). *Business Law Review*, 1, 14-20.
9. Kosegeran, G. (2022). Perlindungan Hukum Penggunaan Data Pribadi Oleh Pihak Lain Tanpa Izin. *Lex Privatum*, 9(12).
10. Manurung, E. A. P., & Thalib, E. F. (2022). Tinjauan Yuridis Perlindungan Data Pribadi Berdasarkan Uu Nomor 27 Tahun 2022. *Jurnal Hukum Saraswati (JHS)*, 4(2), 139-148.
11. Nababan, D., & Lasmadi, S. (2023). Pertanggungjawaban Pidana Terhadap Penyalahgunaan Data Pribadi Pada Tindak Pidana Dunia Maya. *PAMPAS: Journal Of Criminal Law*, 4(2), 232-251.
12. Najla, A., Faisal, F., & Fatahillah, F. (2023). Perlindungan Hukum Terhadap Konsumen Pinjaman Berbasis Online Oleh Otoritas Jasa Keuangan (Ojk) Berdasarkan Pojk Nomor 6/Pojk. 07/2022. *Madani: Jurnal Ilmiah Multidisiplin*, 1(8), 25-37.
13. Nugroho, F. E. (2016). Kemampuan Hukum Dalam Mengantisipasi Perkembangan Teknologi. *Jurnal Paradigma Hukum Pembangunan*, 1(02), 109-118.
14. Pakarti, M. H. A., Farid, D., Saepullah, U., & Sucipto, I. (2023). Pengaruh Perkembangan Teknologi Terhadap Perlindungan Privasi Dalam Hukum Perdata. *SULTAN ADAM: Jurnal Hukum dan Sosial*, 1(2), 204-212.
15. Poernomo, S. L. (2023). Analisis Kepatuhan Regulasi Perlindungan Konsumen dalam E-Commerce di Indonesia. *UNES Law Review*, 6(1), 1772-1782.
16. Priliasari, E. (2023). Perlindungan Data Pribadi Konsumen Dalam Transaksi E-Commerce. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 12(2).

17. Rahman, F. (2021). Kerangka Hukum Perlindungan Data Pribadi Dalam Penerapan Sistem Pemerintahan Berbasis Elektronik Di Indonesia. *Jurnal Legislasi Indonesia*, 18(1), 81-102.
18. Ranto, R. (2019). Tinjauan Yuridis Perlindungan Hukum Terhadap Konsumen Dalam Transaksi Jual Beli Melalui Media Elektronik. *Jurnal Ilmu Hukum: ALETHEA*, 2(2), 145-164.
19. Saly, J. N., & Sulthanah, L. T. (2023). Pelindungan Data Pribadi dalam Tindakan Doxing Berdasarkan Undang-Undang Nomor 27 Tahun 2022. *Jurnal Kewarganegaraan*, 7(2), 1708-1713.
20. Silalahi, P. H., & Dameria, F. A. (2023). Perlindungan Data Pribadi Mengenai Kebocoran Data Dalam Lingkup Cyber Crime Sebagai Kejahatan Transnasional. *Wajah Hukum*, 7(2), 614-627.
21. Soekanto, S. (2007). Penelitian hukum normatif: Suatu tinjauan singkat.
22. Sulistianingsih, D., Ihwan, M., Setiawan, A., & Prabowo, M. S. (2023). Tata kelola perlindungan data pribadi di era metaverse (telaah yuridis undang-undang perlindungan data pribadi). *Masalah-Masalah Hukum*, 52(1), 97-106.
23. Tektona, R. I., & Roziqin, C. (2020). Kepastian Hukum Kewenangan Otoritas Jasa Keuangan Terhadap Kepailitan Lembaga Perbankan Menurut Undang-Undang Nomor 21 Tahun 2011 Tentang Otoritas Jasa Keuangan. *PALAR (Pakuan Law Review)*, 6(01).
24. Yudistira, M., & Ramadani, R. (2023). Tinjauan Yuridis Terhadap Efektivitas Penanganan Kejahatan Siber Terkait Pencurian Data Pribadi Menurut Undang-Undang No. 27 Tahun 2022 oleh KOMINFO. *UNES Law Review*, 5(4), 3917-3929.