

The Impact of the Personal Data Protection Law on Digital Marketing Strategies in Banking Companies

Ni Nyoman Muryatini¹ | Ni Wayan Cahya Ayu Pratami¹ | I Gusti Ngurah Gede Gitayogi Irhandi¹

1. Information Systems Study Program, Faculty of Informatics and Computer, Institute of Technology and Business STIKOM Bali, Indonesia

Muryatini, N, N., Pratami, N, W, C, A., Irhandi, I, G, N, G, G. (2025). The Impact of the Personal Data Protection Law on Digital Marketing Strategies in Banking Companies. *Jurnal Hukum Prasada*, 12(2), 171-177

Abstract

The banking industry went through a rapid digital transformation. The widespread use of digital technology in marketing also presents new challenges related to personal data protection. Banking companies will need to adjust their marketing strategies to be effective but also adhere to data-protection regulations. Personal data protection laws can be a challenge to companies, but they also open opportunities to build customer trust through strong privacy practices. The method used in the study was empirical juridical by using a qualitative approach that produced analytical data based on observation, and questionnaire's analysis. The purpose of this study is to observe firsthand the facts in the field of how law is applied in society. According to research, the personal data protection law (UUPDP) significantly transformed the landscape of digital marketing strategies for Indonesian banking companies. While it presents challenges in compliance, agreement management, and risk penalties, the UUPDP also opens up opportunities to build stronger trust, encourage innovation in marketing approaches, and improve overall data governance. Ironically, after the UUPDP has been legalized for more than two years, the formation of the private data protection agency has yet to be realized, resulting in the realization of the rights of the data subject as well as in law enforcement. It is incompatible with the spirit of the constitution and the UUPDP to ensure the fulfillment of the rights of data subjects as part of human rights. For legal certainty and ensuring the fulfillment of the rights of data subjects (customers), the government must immediately enforce the UUPDP regulation as one that regulates the technical matter.

Article History

Received: July 21, 2025

Accepted: October 13, 2025

Keywords: *banking; marketing strategies; the UUPDP*

Introduction

Protection of personal data is part of human rights that must be guaranteed and protected by the state as mandated by the constitution and laws. Personal data has become a valuable asset for companies, including banks. This data is used for a variety of purposes, from personalizing services to developing new products. More and more countries are enacting stricter personal data protection laws, demonstrating a growing awareness of the importance of protecting individual privacy. The banking industry went through a rapid digital transformation. The use of digital technology in marketing is expanding, but it also presents new challenges related to personal data protection. Banking companies need to adapt their marketing strategies to remain effective while still complying with data protection regulations. Personal data protection laws can be challenging for companies, but they also offer opportunities to build customer trust through strong privacy practices.

Correspondence regarding this article should be addressed to:

Ni Nyoman Muryatini, Faculty of Informatics and Computer, Institute of Technology and Business STIKOM Bali, Indonesia

Email address: tiniaryadiputra2016@gmail.com



Published by Universitas Warmadewa. This is an open access article under the CC-BY SA license

Bank marketing strategies in the digital era cannot avoid the impact of technological change. Consumers are now shifting to faster, easier, and more convenient digital banking services. This is driving banks to continuously develop marketing strategies that can effectively reach consumers through digital platforms. These range from utilizing social media to strategic partnerships with companies and markets in fintech, all strategies implemented are aimed at marketing success in the digital era. According to Hendra, in Eko Juliani and Hendri Riofila, business activities now take place in a digital ecosystem that connects many parties, enabling faster and more efficient interactions and transactions. This digital environment creates new opportunities in marketing and communication, making the business world more dynamic. People demand faster and more convenient services because they provide more internet access. Digital transformation is a solution for the business world, especially banking, to remain competitive in the modern era (Juliana & Riofita, 2024). The banking industry is experiencing rapid digital transformation, and the use of digital technology in marketing is increasingly widespread.

Coviello, Milley, and Marcolin state that digital marketing is the use of the internet and other interactive technologies to create and connect dialogues between companies and identified consumers (Sawhani, 2021). Furthermore, according to Ridwan Sanjaya and Josua Tarigan, digital marketing is a marketing activity including branding that uses various web-based media (Febriyanto & Arisandi, 2018). E-Marketing or digital marketing is defined as the use of digital technology to achieve marketing goals, as well as efforts to develop or adjust the marketing concept itself, can communicate on a global scale, and change the way companies do business with customers. Based on this statement, it can be concluded that digital marketing is a marketing activity that utilizes the internet and digital technology in the process of achieving its marketing goals. Banking marketing is a series of activities undertaken by banks to better understand their customers. Within this marketing strategy, banks also develop products tailored to their needs and plan marketing campaigns to reach customers. The goals of marketing in the banking industry include building brand awareness, product promotion, as well as market analysis and adaptation. Some of the bank's digital marketing strategies are (Tasim, 2024):

- Use of social media;
- Strategic partnership with companies, fintech, and marketplace;
- Implementation of AI and chatbots;
- Utilization of big data for consumer behavior analysis;
- Implementation of search engine optimization;
- Email marketing;
- Paid advertising;
- ASO implementation for applications mobile banking;
- Video marketing;
- Influencer marketing.

The rapid development of technology, information, and communication has created various opportunities and challenges. According to a report by Badan Siber dan Sandi Negara (BSSN) or the National Cyber and Crypto Agency, Indonesia will face significant data breaches by 2023, including in the financial sector, with 165,000 data points exposed. Leaked financial data can include banking information, financial transactions, and customer personal details, which can potentially be used by irresponsible parties to commit fraud and identity theft (Iswenda, 2024). Personal data has become a valuable asset for companies, including banks. This data is used for various purposes, from personalizing services to developing new products. Banking companies need to adapt their marketing strategies to remain effective while still complying with data protection regulations. Personal data protection laws can be challenging for companies, but they also offer opportunities to build customer trust through strong privacy practices. As more countries enact stricter personal data protection laws, this demonstrates a growing awareness of the importance of protecting individual privacy.

Method

This study employed empirical juridical research, which directly observes the facts on the ground and how law is applied in society (Efendi & Ibrahim, 2018). A qualitative approach was employed, producing descriptive analytical data based on observations and questionnaires from 50 respondents. Random sampling was used as the sampling technique.

Discussion

The Impact of Personal Data Protection Law on Digital Marketing Strategies in Banking Companies

According to Law Number 27 of 2022 concerning Personal Data Protection (*UU PDP*), personal data is data about an individual that is identified or identifiable individually or in combination with other information, either directly or indirectly, through electronic or non-electronic systems. Personal data consists of specific personal data and general personal data. Specific personal data includes: health data and information, biometric data, genetic data, criminal records, child data, personal financial data, and other data in accordance with laws and regulations. Meanwhile, general personal data includes: full name, gender, nationality, religion, marital status, and personal data combined to identify an individual.

The *UU PDP* has a significant impact on the digital marketing strategies of banking companies. Banking companies must ensure that all digital marketing activities they implement comply with *UU PDP* regulations. This includes obtaining explicit consent from customers before collecting, storing, or using their personal data. Failure to comply can result in serious legal sanctions. Banking companies' legal compliance with the *UU PDP* is crucial for maintaining customer trust and ensuring that their personal data is properly protected. Banking companies must have a clear and transparent privacy policy that explains how customer personal data is collected, used, and protected. Customers must be provided with easily understandable information regarding their rights regarding their personal data. Banks must obtain customer consent before collecting or processing their personal data. This consent must be given voluntarily and based on sufficient information. Implement strict security measures to protect personal data from unauthorized access, loss, or leakage. This includes the use of encryption technology, firewalls, and intrusion detection systems.

Banks should provide training to employees on the importance of protecting personal data and how to handle it securely. This is to ensure that all staff understand the applicable policies and procedures. Appoint a Data Protection Officer (DPO) responsible for overseeing compliance with the *UU PDP* and liaising with data protection authorities. Conducting regular risk assessments to identify potential threats to personal data and taking necessary mitigation measures. Conducting internal and external audits to ensure that all data protection policies and procedures are adhered to and are effective. Providing customers with the right to access their personal data and correcting inaccurate information. Having procedures in place to notify customers and relevant authorities in the event of a data breach that could compromise customer personal data. Adhering to these steps, banking companies can ensure they meet applicable legal requirements and adequately protect customer personal data.

With the existence of the *UU PDP*, companies, particularly in the banking sector, need to be more transparent about how they collect, store, and use customer data. This transparency not only helps comply with legal regulations but also increases customer trust in banks. This trust is crucial because it can strengthen the relationship between customers and banks, increase loyalty, and ultimately contribute to the company's long-term success. Furthermore, by demonstrating a commitment to data protection, banks can differentiate themselves from competitors and attract more customers who are increasingly aware of the importance of data privacy. Banks must adopt better data management practices to ensure that customers' personal data is properly protected. This includes the use of encryption technology and robust security protocols. Adopting better data management practices is crucial to protecting customers' personal data. Some steps companies can take include:

- Using encryption technology to ensure that sensitive data cannot be accessed by unauthorized parties.

- Implement strong security protocols, such as HTTPS, to protect data during transmission.

- Limit access to personal data to only those employees who need it for their jobs.

- Provide cybersecurity training to employees to raise awareness about the importance of data protection.

- Ensure that all systems and software are regularly updated to address newly discovered security vulnerabilities.

- Conduct regular risk assessments to identify and mitigate potential threats to personal data.

Taking these steps will enable companies to improve data security and build trust with customers.

While customer data can be used to personalize services, banks must be careful not to violate customer privacy. Marketing strategies must be designed with respect to privacy boundaries while still providing added value to customers. When designing marketing strategies that utilize customer data, banks must balance personalization and privacy. It is important to ensure that customer data is used ethically and in accordance with applicable privacy regulations, such as: the General Data Protection Regulation in the European Union or the CCPA in California. Transparency about how data will be used, as well as providing customers with options to control their data, can help build trust and ensure that marketing strategies are not only effective but also respect the rights of bank customers.

Banks need to adapt their marketing strategies to reduce their reliance on personal data. This could involve using anonymized or aggregated data, as well as exploring alternative marketing methods that don't rely on personal data. With increasing privacy concerns and stricter regulations regarding the use of personal data, banks need to explore more sustainable and ethical marketing strategies. Here are some approaches to consider:

Anonymizing data allows companies to still gain valuable insights without compromising individual privacy. Aggregated data can also provide a broader view of trends without specifically targeting individuals.

Contextual marketing targets ads based on the content that users are currently viewing. This can be an effective way to reach relevant audiences without violating privacy.

Explicitly requesting permission from users before collecting or using their data ensures that companies respect user privacy and builds trust.

Building strong communities and offering quality content can increase customer engagement and loyalty without the need to rely on personal data.

Utilizing technologies such as artificial intelligence to analyze overall market trends can provide useful insights without the need for personal data.

In adopting these strategies, banks can reduce their reliance on personal data and still undertake effective and ethical marketing campaigns.

Banks need to invest time and resources in training employees on the importance of data protection and how to comply with personal data protection regulations. This includes understanding customers' rights regarding their personal data. Overall, while this law may increase challenges for banking companies in their digital marketing strategies, it also offers opportunities to build stronger and more trusted relationships with customers.

Article 46 of the *UUPDP* states that, in the event of a failure in protecting personal data, the bank as the controller of personal data is required to provide written notification to the personal data subject (customer) within 3 x 24 hours. The written notification shall contain the personal data disclosed, when and how the personal data was disclosed, and the bank's efforts to handle and recover from the disclosure of personal data. In certain cases, the bank is required to notify the public of the failure to protect personal data. In this case, the bank is required to be responsible for the processing of personal data and demonstrate accountability in fulfilling its obligations to implement the principles of personal data protection.

Article 58 of the *UUPDP* mandates the immediate establishment of a personal data protection agency. However, more than two years after the *UUPDP* was passed, no such agency has been established. This agency's duties include:

Implementing the formulation and determination of personal data protection policies and strategies that serve as guidelines for personal data subjects, personal data controllers, and personal data processors.

Carrying out supervision of the implementation of personal data protection.

Implementing administrative law enforcement against violations of *UUPDP*.

Implementing out-of-court dispute resolution facilitation.

Furthermore, Article 60 emphasizes the 15 authorities of this institution, namely establishing policies, monitoring compliance of personal data controllers, receiving complaints of alleged violations, and imposing administrative sanctions. If compliance standards have not been established because the institution has not been established, fulfilling the rights of data subjects is difficult to implement. The

compliance standards that must be met by the industry are also unclear, this will certainly impact law enforcement. The implication of this is that the provisions in the *UUPDP*, which are further regulated in its derivative regulations, cannot be implemented, because there is no reference in the form of regulations that regulate the technical matters. Considering that the protection of personal data is a human right, the state must be responsible for guaranteeing legal protection for all citizens by immediately ratifying regulations derived from the *UUPDP*.

Legal Awareness of Banking Customers Understands the Importance of Personal Data Protection

Banking customers' legal awareness regarding personal data protection is becoming increasingly important in this digital era. Customers must understand their rights and obligations regarding personal data protection to protect sensitive information from misuse.

Customers should be aware of what data falls under the category of personal data, such as name, address, identity number, and financial information. Bank customers' understanding of personal data is crucial in the context of privacy protection and information security. Customers should understand the types of personal data collected by banks, such as name, address, telephone number, email address, financial information, and other identifying data. Customers need to understand the purpose of personal data collection. Banks typically collect data to verify identity, process transactions, provide banking services, and comply with laws and regulations. Customers have the right to know how their data is used, request access to their personal data, and correct inaccurate data. Customers also have the right to request data deletion in certain situations. It is important for customers to understand the steps taken by the bank to protect their personal data from unauthorized access, such as data encryption and information security policies. Customers should be informed if their personal data will be shared with third parties and for what purpose. Customer consent may be required before data is shared. Customers should read and understand the bank's privacy policy to understand how their personal data is managed and protected. Customers should be aware of their bank's procedures in the event of a data breach, including how they will be notified and the steps taken to address the breach. By understanding these issues, customers can be more proactive in protecting their personal data and making informed decisions about the banking services they use.

Customers have the right to know how their data is used, stored, and shared by banking institutions, and also have the right to request access, correction, or deletion of their personal data if necessary. Banking customers' rights to personal data protection are an important aspect that must be upheld by financial institutions. Customers have the right to receive clear and transparent information regarding how their personal data will be used, stored, and protected by the bank. Customers must provide explicit consent before personal data is collected or used for a specific purpose. Banks must ensure that this consent is given voluntarily and based on sufficient information. Customers have the right to access their personal data held by the bank, request a copy of that data, and learn how it is used. If the personal data held by the bank is inaccurate or incomplete, customers have the right to request correction or updating of that data. Under certain circumstances, customers have the right to request deletion of their personal data, for example, if the data is no longer necessary for the original purpose of collection. Customers may request restriction of the processing of their personal data in certain situations, such as when they contest the accuracy of the data or when the data is no longer necessary for the purpose of processing. Customers have the right to request that their personal data be transferred to another service provider in a machine-readable format. Customers have the right to object to the processing of their personal data for certain purposes, such as direct marketing. Customers have the right to protection against unauthorized access, disclosure, or use of their personal data. Customers have the right to file a complaint with a data protection authority if they believe their rights have been violated. Banks and other financial institutions are required to comply with applicable personal data protection regulations in Indonesia.

Banking institutions are required to implement adequate security measures to protect customers' personal data from unauthorized access, leakage, or theft. Banking institutions have a significant responsibility to protect customers' personal data. Adequate security measures can include data

encryption, the use of strong authentication systems, monitoring for suspicious activity, and cybersecurity training for employees. Furthermore, it is crucial for banking institutions to ensure they comply with applicable data protection regulations and standards in Indonesia. Therefore, customers can feel more secure and confident in transacting with these institutions.

Customers should read and understand their bank's privacy policy before providing any personal data. This policy typically explains how data is collected, used, and protected. Reading and understanding a bank's privacy policy is crucial to ensure customers understand how their personal data will be managed. Privacy policies typically include information about the types of data collected, the purposes for which that data will be used, and the steps the bank takes to protect data from unauthorized access or misuse. Understanding these policies can make customers more informed about the decisions and feel more secure in their interactions with the bank.

Customers should immediately report any suspected personal data protection violations to the relevant authorities or agencies. Reporting suspected personal data protection violations to the relevant authorities or agencies is a crucial step in protecting customer rights. Reporting the incident allows authorities to investigate and take necessary action to prevent further data misuse. Furthermore, it helps raise awareness and encourage better data protection practices in the future. Law enforcement against personal data breaches faces significant challenges, particularly related to government oversight and business actors' legal awareness.

Table 1. Questionnaire Calculation Results

No	Description	Percentage
1	Knowing the Personal Data Protection Law	96%
2	The influence of the UUPDP on bank marketing strategies	58%
3	Satisfied with personal data security	46%
4	Not sure if the bank provides information about personal data protection	22%
5	Personal data leaked	14%
6	Expect increased security and protection of personal data	90%

A questionnaire distributed to 50 commercial bank customers in Denpasar City, stated that 96% of respondents were aware of *UUPDP* but did not understand it in depth, information was obtained from bank websites, social media and television media. As many as 58% stated that *UUPDP* is very influential on the landscape of bank marketing strategies, 46% stated that they were satisfied with the protection of personal data, 22% stated that they were not sure that banks provided information about personal data protection, because more often they only provided information about bank products and services, 14% stated that they had experienced personal data leaks, and 90% expected an increase in the security and protection of personal data, because often customer data was given to third parties such as insurance and credit cards that had never been asked for approval from customers.

The government's active role in disseminating information and educating about the *UUPDP* is crucial. Increasing education and awareness regarding personal data protection through seminars, workshops, or public campaigns can help banks and customers become more vigilant and proactive in protecting their personal data. Increasing education and awareness regarding personal data protection is crucial in this digital age. Customers can gain better information about the risks and how to protect their personal data by holding seminars, workshops, or public campaigns. It can also help customers understand their rights regarding data privacy and the steps that can be taken to prevent misuse of personal data. As such, people will become more vigilant and proactive in protecting their personal information from potential threats. With increased legal awareness and understanding of the importance of personal data protection, customers can be better protected from potential financial and privacy risks.

Conclusion

The Personal Data Protection Law (*UUPDP*) significantly changes the digital marketing strategy

landscape for banking companies in Indonesia. While it poses challenges in terms of compliance, consent management, and the risk of fines, the Personal Data Protection Law also opens up opportunities to build stronger customer trust, encourage innovation in marketing approaches, and improve overall data governance. Banking customers' legal awareness regarding personal data protection is becoming increasingly important in this digital era. Customers must understand their rights and obligations regarding personal data protection to protect sensitive information from misuse. Banking companies must ensure that all digital marketing activities comply with the UUPDP regulations, including obtaining explicit customer consent before collecting, storing, or using personal data. Failure to comply can result in serious legal sanctions. Banking companies' legal compliance with personal data protection laws is a crucial aspect of maintaining customer trust and ensuring that customer personal data is properly protected. Ironically, more than two years after the establishment of the Personal Data Protection Law, the establishment of a personal data protection agency has yet to be implemented. This impacts the fulfillment of data subjects' (customers) rights and law enforcement. This contradicts the spirit of the constitution and the UUPDP, which guarantee the fulfillment of data subjects' rights as part of human rights.

References

- Efendi, J., & Ibrahim, J. (2018). *Metode Penelitian Hukum: Normatif dan Empiris*. Jakarta : Kencana
- Febriyantoro, M. T., & Arisandi, D. (2018). Pemanfaatan Digital Marketing Bagi Usaha Mikro, Kecil Dan Menengah Pada Era Masyarakat Ekonomi Asean. *JMD: Jurnal Riset Manajemen & Bisnis Dewantara*, 1(2), 61-76. <https://doi.org/10.26533/jmd.v1i2.175>
- Hasibuan, E. S., & Salsiah, L. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi Terhadap Kejahatan Pelanggaran Data Di Indonesia. *Jurnal Pro Hukum : Jurnal Penelitian Bidang Hukum Universitas Gresik*, 11(3), 63–69. Retrieved from <https://journal.unigres.ac.id/index.php/JurnalProHukum/article/view/2072>
- Iswenda, B. A (2024). Jumlah Kebocoran Data di Indonesia Capai 1 Juta di 2023. *goodstats.id*. Retrieved from <https://goodstats.id/article/data-yang-tersebar-secara-tidak-sah-pada-2023-hampir-mencapai-1-juta-data-Rh2qg>
- Juliana, E., & Riofita, H. (2024). Livin' by Mandiri Sebagai Strategi Pemasaran PT. Bank Mandiri. *Jurnal Nasional Manajemen Pemasaran Dan SDM*, 5(3), 342 - 349. <https://doi.org/10.47747/jnmpsdm.v5i3.2243>
- Lesmana, C. T., Elis, E., & Hamimah, S. (2022). Urgensi Undang-Undang Perlindungan Data Pribadi Dalam Menjamin Keamanan Data Pribadi Sebagai Pemenuhan Hak Atas Privasi Masyarakat Indonesia. *Jurnal Rechten : Riset Hukum Dan Hak Asasi Manusia*, 3(2), 1-6. <https://doi.org/10.52005/rechten.v3i2.78>
- Sawlani, D. K. (2021). *Digital Marketing: Brand Images*. Surabaya : Scopindo Media Pustaka.
- Tasim, C. (2024). 10 Strategi Marketing Perbankan di Era Digital untuk Meningkatkan Daya Saing. *toffeedev.com*. Retrieved from <https://toffeedev.com/blog/digital-marketing/strategi-marketing-perbankan-di-era-digital/>