JURNAL MAGISTER HUKUM UDAYANA
(UDAYANA MASTER LAW JOURNAL)
Vol. 14 No. 4 December 2025
E-ISSN: 2502-3101 P-ISSN: 2302-528x
http: //ojs.unud.ac.id/index.php/jmhu

The Legal Framework for Personal Data Deletion on Social Media in Indonesia: A New Chapter in Digital Privacy Protection

I Putu Gede Arya Sanjaya[1], Dewa Krishna Prasada[2]

[1]Fakultas Hukum Universitas Pendidikan Nasional, E-mail: aryasanjaya2004@gmail.com
[2]Fakultas Hukum Universitas Pendidikan Nasional, E-mail: krisnaprasada@undiknas.ac.id

Article Info
Receiverd: 24th August 2025
Accepted: 22nd December 2025
Published: 30th December 2025

Keywords:
Legal Framework; Personal Data Deletion; Social Media.

Corresponding Author:
I Putu Gede Arya Sanjaya, E-mail: aryasanjaya2004@gmail.com

DOI:
10.24843/JMHU.2025.v14.i04.p01

Abstract
The pervasive use of social media necessitates serious attention to personal data protection, particularly during registration where users must provide identifiers like usernames, birth dates, and email addresses, raising significant legal concerns over data security and management. In Indonesia, this protection is framed by Law No. 27 of 2022 on Personal Data Protection (PDP Law). Article 8 explicitly affirms the data subject's right to terminate processing, delete, and/or destroy personal data, formally acknowledging the right to erasure. However, the law omits clear technical procedures for exercising this right, creating legal uncertainty. This study aims to address two primary questions: first, how current positive law (ius constitutum) regulates social media users' personal data protection regarding personal data deletion; and second, the legal responsibilities of platforms in personal data breach cases. Employing normative legal research with a descriptive-analytical library approach, the study utilizes statutory and analytical methods. Legal materials comprise primary sources like regulations and secondary sources including legal textbooks and journals. Data is presented, interpreted, and evaluated through qualitative descriptive-analytical analysis. The research findings indicate that the process for personal data deletion on social media platforms remains heavily contingent upon user-agreed terms and conditions, governed by contractual agreements. Furthermore, platforms bear legal responsibility to provide compensation, specifically in the form of monetary damages, for breaches resulting from their proven fault or negligence.

I. Introduction

The establishment of a robust legal framework for personal data deletion on social media in Indonesia marks a pivotal new chapter in the nation's digital privacy protection. This development is fundamentally rooted in Indonesia's unique constitutional and philosophical foundations. The national legal concept is not derived from a vacuum but is intrinsically built upon the state ideology of Pancasila and the 1945 Constitution of the Republic of Indonesia (UUD 1945). Pancasila, particularly its

second principle of "Just and Civilized Humanity," provides the ethical bedrock, emphasizing the protection of human dignity—a concept that extends inherently to privacy and personal autonomy in the digital age. This philosophical mandate is concretized in the Constitution. While the UUD 1945 does not explicitly mention "privacy" or "personal data," Article 28G paragraph (1) powerfully guarantees that "Every person shall have the right to the protection of his/herself, family, honour, dignity, and property," which has been widely interpreted by legal scholars and the Constitutional Court to encompass the right to privacy. Furthermore, Article 28D paragraph (1) assures legal certainty. Therefore, the regulation of data deletion is a direct legislative manifestation of these supreme values, translating abstract constitutional protections into actionable rights, ensuring that the digital realm respects the human dignity and legal certainty mandated by Indonesia's highest laws.

The concept of personal data protection has undergone significant transformation over time, particularly in response to technological advancements in the digital era. At its core, personal data protection refers to legal and technical measures designed to secure individuals' privacy in relation to the collection, processing, storage, and dissemination of their personal information Historically, the modern understanding of personal data protection began to take shape in the early 20th century. A notable milestone was the introduction of the Social Security Number (SSN) in the United States in 1936, originally created to administer social benefits but gradually evolving into a universal identifier. By the 1970s, legal efforts to regulate data usage became more pronounced with the enactment of the Privacy Act of 1974 in the United States, as well as data protection developments in Europe, including references in the European Convention on Human Rights.[1]

In the 1980s, the proliferation of computer technology prompted several countries to enact their first generation of data protection legislation. The United Kingdom, for instance, introduced the Data Protection Act of 1984, although the scope of such laws remained relatively limited. The legal landscape evolved further in the 1990s with the European Union's Data Protection Directive (Directive 95/46/EC), which mandated member states to implement national data protection laws aligned with common principles—laying the groundwork for the subsequent General Data Protection Regulation (GDPR).[2]

The early 2000s witnessed rapid digitalisation and global internet penetration, generating unprecedented volumes of personal data and increasing concern over digital privacy. Legal reforms during this period—particularly updates to the U.S. Privacy Act—sought to reflect the complexities of data handling in an interconnected world. A major turning point arrived in 2018 with the enactment of the GDPR, which redefined global data protection standards by enhancing user rights and imposing stricter obligations on data controllers and processors (Saputri, 2023). Globally, various jurisdictions followed suit by implementing comparable frameworks. Canada adopted the Personal Information Protection and Electronic Documents Act (PIPEDA), Australia

[1] CYMONE GOSNELL, 'The General Data Protection Regulation: American Compliance Overview and the Future of the American Business.' (2019) 15(1) *Journal of Business & Technology Law* 165 <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=142055261&site=ehost-live>.

[2] Ibid.

enacted the Privacy Act, and Japan updated its Act on the Protection of Personal Information. These regulatory regimes, while differing in scope and enforcement, collectively emphasised the need for robust legal safeguards in a data-driven environment.

The historical trajectory of Information Technology (IT) law in Indonesia demonstrates an adaptive, often reactive, legislative response to technological advancement. Initial frameworks in the late 1990s and early 2000s focused on telecommunications infrastructure, leaving a significant regulatory void for the digital realm. This gap was first substantively addressed by the landmark Law No. 11 of 2008 on Electronic Information and Transactions (ITE Law), which established the legal validity of electronic evidence, signatures, and transactions. However, its broad provisions, especially on online defamation (Article 27(3)), sparked continuous debate and misuse. A significant amendment came with Law No. 1 of 2024, which refined several contentious articles to provide greater legal certainty, emphasize the principle of actus reus (guilty act) for violations, and strengthen procedural safeguards for law enforcement. This evolution, culminating in the comprehensive Personal Data Protection Law of 2022, illustrates

In Indonesia, the enactment of Law No. 27 of 2022 on Personal Data Protection (PDP Law), signed by President Joko Widodo on 17 October 2022, marked a historic milestone in aligning national data protection laws with global standards such as the GDPR. Prior to this, Regulation of the Minister of Communication and Informatics No. 20 of 2016 had addressed aspects of data protection but lacked comprehensive classification and enforcement mechanisms. The PDP Law introduces a clearer taxonomy of key actors and types of personal data. It distinguishes between General Personal Data—such as name, gender, nationality, and marital status—and Special Personal Data, which includes biometric, genetic, health, financial, and criminal records, as well as data concerning children. The law also defines the roles of Data Subjects, Data Controllers, and Data Processors, thereby establishing accountability across the data lifecycle.[3]

Moreover, Article 8 of the PDP Law explicitly grants data subjects the right to request the termination of processing, deletion, and/or destruction of their personal data, reinforcing individual autonomy. However, the law presents normative ambiguities, particularly regarding the procedural mechanism for executing such rights, which remains under-regulated. This legal vacuum becomes especially problematic in light of repeated data breach incidents in Indonesia, such as the 2022 case involving the alleged leak of 105 million citizens' data from the General Elections Commission (KPU) database and the breach of BPJS Kesehatan data. These incidents underscore the urgent need for enforcement clarity, judicial recourse, and a reliable technical framework for data erasure requests.[4]

As online transactions and platform-based services proliferate, the governance of personal data increasingly relies on "Terms and Conditions" agreements between users and service providers. These documents often serve as the legal foundation that defines rights, responsibilities, and permissible use of personal data. Yet, the asymmetry of

[3] Muhammad Fajri Fernando, 'Perlindungan Hukum Terhadap Data Pribadi Konsumen Pada Perdagangan Elektronik (E-Commerce)' (2016).

[4] Alga Soraja, 'Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Prespektif HAM' [2021] *Prosiding Seminar Nasional Kota Ramah Hak Asasi Manusia* 20.

power and knowledge between users and platforms calls for stricter legal intervention to ensure that user consent is informed, voluntary, and revocable. In conclusion, Indonesia's legal framework for personal data protection is evolving in response to both international trends and domestic challenges. While Law No. 27 of 2022 represents significant progress, its successful implementation depends on comprehensive regulations, effective enforcement, and public awareness.

In the context of Article 8 of the PDP Law, "normative ambiguity" manifests as a procedural vacuum. The law only stipulates what the right is—namely the right to delete data—but does not regulate how the mechanism for exercising this right should be implemented. This vacuum creates legal uncertainty and inconsistency in practice. Each data controller (such as social media platforms, e-commerce sites, or banks) is authorized to establish different deletion request procedures, without any clear, standardized framework. Consequently, the burden of navigating and complying with these diverse procedures falls entirely on the public as data subjects. Based on this background, this research seeks to answer two main legal questions. First, how does the applicable legal framework (*ius constitutum*) regulate the protection of social media users' personal data, specifically regarding the legal basis and mechanisms for personal data deletion? Second, what is the form and scope of legal responsibility that social media platforms must bear in the event of a breach or leakage of users' personal data?.

2. Research Method

This study employs a normative legal research methodology, emphasizing the use of legal literature as the primary source to address the identified legal issues. The research adopts a comparative approach, in addition to the statutory and analytical approaches, to examine the legal framework surrounding the deletion of personal data on social media platforms. This is done particularly within the context of Indonesian law as stipulated in Article 8 of Law No. 27 of 2022 on Personal Data Protection and contrasted with relevant frameworks from other jurisdictions. The comparison will focus on two main legal traditions: first, jurisdictions that use the term "personal data" and offer detailed procedural models, such as the European Union's General Data Protection Regulation (GDPR); and second, jurisdictions that employ the term "personal information," including the United States (notably under the California Consumer Privacy Act - CCPA), Canada (under PIPEDA), and Australia (under its Privacy Act). The motivation for this research arises from the absence of explicit procedural regulations concerning data deletion in the aforementioned Article, which creates normative ambiguity. Accordingly, this gap serves as the foundation for the researcher's inquiry. To address the research questions, a descriptive-analytical method guides the analysis. The normative issues are first delineated based on a review of relevant legal sources. This foundation then allows for a phase of interpretation and evaluation, where the materials are critically examined to build logical conclusions tailored to the specific legal problems at hand.[5]

3. Results and Discussion

[5] Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi* (Kencana, 2017).

3.1 Regulatory Framework for Protecting Social Media Users' Personal Data in Relation to Data Deletion

In the realm of personal data protection, different nations apply varying terminologies to describe similar concepts. For instance, jurisdictions such as the United States, Canada, and Australia typically refer to the term "personal information," whereas countries within the European Union, as well as Hong Kong, Malaysia, and Indonesia, predominantly use "personal data." The terminology used to define information that relates to an identifiable individual varies significantly across jurisdictions, reflecting diverse legal traditions and philosophical approaches to privacy. In common law countries like the United States, Canada, and Australia, the prevailing term is "personal information." This terminology is embedded in key legislations such as the U.S. California Consumer Privacy Act (CCPA), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), and Australia's Privacy Act 1988. The concept of "personal information" often carries a contextual and sometimes broader connotation, focusing on information that can be linked to an individual within a specific circumstance. In contrast, many other jurisdictions, particularly those influenced by European civil law traditions, consistently employ the term "personal data." This is the standard terminology within the European Union, as enshrined in the General Data Protection Regulation (GDPR), which has serve—"personal information" and "personal data"—can be substantially similar, the linguistic divergence signifies deeper jurisprudential nuances. The choice of terminology can subtly influence interpretive approaches, the categorization of information, and the alignment with international data transfer mechanisms, making it a critical point of analysis in comparative data privacy law.

Despite these linguistic distinctions, both expressions refer to any information connected to a specific individual that may be used, either independently or in conjunction with other data, to identify that individual. Essentially, personal data denotes any details—whether stored digitally or otherwise—that could directly or indirectly pinpoint a person's identity.[6]

In Indonesia, the definition of personal data is encapsulated in the Regulation of the Minister of Communication and Informatics Number 20 of 2016 on the Protection of Personal Data in Electronic Systems (Permenkominfo 20/2016). According to Article 1, point 1 of this regulation, personal data encompasses particular individual information that is stored, preserved, and maintained to uphold its confidentiality. This legal articulation underscores the importance of safeguarding and managing data privacy, especially within the context of digital systems. Comparatively, the General Data Protection Regulation (GDPR) of the European Union defines personal data as any form of information linked to an identifiable natural person, whether through direct indicators such as a name or identification number or indirect cues such as online identifiers, geolocation, or physiological and sociocultural characteristics.[7]

---

[6] Komal Batool Syed Khurrum Hussain Naqvi, 'A Comparative Analysis between General Data Protection Regulations and California Consumer Privacy Act' (2023) 4(1) *Journal of Computer Science, Information Technology and Telecommunication Engineering* 326.

[7] Bagus Satryo Ramadha, 'Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perindungan Data Pribadi Di Indonesia' (Universitas Islam Indonesia, 2021) <chrome-

In the United States, the Personal Data Act of 1998, particularly in Section 3, elaborates that personal data involves any detail that refers, directly or indirectly, to a living individual. This inclusive definition is irrespective of the data's format, highlighting the overarching principle that any information capable of tracing a person's identity falls within the bounds of personal data. This broad interpretation demonstrates the critical role personal data plays in constructing an individual's digital and real-world persona.

From a human rights standpoint, the concept of personal data is deeply intertwined with the fundamental right to privacy. This right encompasses various freedoms such as protection from unwarranted intrusion into private life, secure communication without surveillance, and authority over personal information. Therefore, mishandling or unauthorized use of such data can be considered an infringement upon an individual's privacy rights. Unauthorized access or misuse of personal information without the data subject's consent constitutes a serious breach of privacy. Recognizing and upholding these privacy-related rights requires strict adherence to data governance and compliance with legal frameworks established for personal data protection.[8]

Beyond legal compliance, the safeguarding of personal data represents an ethical commitment that reinforces trust between organizations and individuals. By ensuring that data is processed responsibly and securely, institutions not only comply with statutory obligations but also enhance their credibility and mitigate risks associated with privacy breaches. The potential harm caused by such breaches could affect individuals on both personal and professional levels.

In the Indonesian Personal Data Protection Law (Law No. 27 of 2022), personal data is divided into two primary categories: general and sensitive data. Article 4, paragraph 1 of this law provides clear delineation between these categories, as well as the specific types of information classified under each. General personal data includes details such as name, gender, religion, nationality, and marital status—any information that might reasonably be used to identify an individual. These data sets are often accessible and commonly shared, though they still require legal protection.

In contrast, sensitive personal data necessitates more rigorous protection due to the potentially severe consequences of misuse. This category comprises health-related data, biometric identifiers like fingerprints and retina scans, genetic information, criminal history, children's data, and financial records. The sensitivity of this information means that its exposure could lead to significant personal, professional, or even legal harm to the individual concerned. Moreover, the PDP Law allows for the inclusion of other types of data in this sensitive category based on evolving legal interpretations and regulatory requirements.[9]

Electronic information, as defined by the PDP Law, also falls under the protective umbrella of personal data regulations. This includes a wide array of digital content such as texts, audio recordings, images, designs, maps, emails, codes, symbols, and electronic

---

extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.uii.ac.id/bitstream/handle/123456789/31626/18912046 Bagus Satryo Ramadha.pdf?sequence=1&isAllowed=y>.

[8] Hendrawan Agusta, 'Keamanan Dan Akses Data Pribadi Penerima Pinjaman Dalam Peer to Peer Lending Di Indonesia' (2021) 15(1) *Krtha Bhayangkara* 11.

[9] Muhammad Fajri Fernando, 'Perlindungan Hukum Terhadap Data Pribadi Konsumen Pada Perdagangan Elektronik' [2022] *Jurnal Universitas Muhammadiyah Palembang*.

signatures. Whether stored in electronic systems or represented through digital documents, these materials are considered vulnerable to misuse and thus necessitate stringent protections. Ensuring the confidentiality and integrity of electronic data is paramount in preventing unauthorized access and maintaining the security of individuals' personal information. The classification into general and sensitive categories facilitates the establishment of tiered security protocols tailored to the level of risk associated with each type of data. This strategic legal differentiation aims to ensure that high-risk data receives enhanced security treatment, which is essential in protecting the dignity, rights, and welfare of data subjects. Hence, Indonesia's PDP Law lays out a holistic framework for data governance that not only defines and categorizes data but also prescribes mechanisms for lawful and ethical data processing.[10]

The discourse on social media cannot be separated from the concept of legal agreements, especially concerning user consent. In Indonesian civil law, specifically Article 1313 of the Civil Code (KUHPer), an agreement is defined as an act in which one or more parties bind themselves to one or more other parties. This is further interpreted by legal scholar R. Subekti as a mutual promise between individuals that creates legally enforceable obligations. Agreements form the legal backbone of user-provider relationships on digital platforms, including terms and conditions that dictate how user data is managed.

For an agreement to be considered valid under Indonesian law, four essential elements must be fulfilled as outlined in Article 1320 of the Civil Code. These include: (a) mutual consent of the parties, (b) legal competence of the parties involved, (c) a specific and identifiable subject matter, and (d) a lawful objective. Mutual consent must be free of coercion or misrepresentation, while legal competence requires that individuals have reached the age of majority or are otherwise deemed legally capable. The agreement must relate to a clearly defined object, and the objective of the contract must not contravene statutory regulations, public order, or morality.

Understanding these legal requirements is crucial in evaluating user agreements on social media platforms, particularly concerning data rights. When users agree to terms of service, they are effectively consenting to the platform's data handling policies. Therefore, transparency and fairness in drafting these terms are essential to avoid exploitative practices and uphold user rights. One social media platform that illustrates this dynamic is TikTok. According to the platform's data privacy policy—specifically the section titled "Your Rights and Your Choices"—users are informed of their entitlements concerning their personal data. These include rights granted under relevant data protection laws, such as the ability to access, delete, update, or correct personal data. Additionally, users can inquire about how their data is processed, lodge complaints with relevant authorities, and appeal decisions made by TikTok concerning their data-related requests.[11]

TikTok establishes clear provisions regarding personal data protection by providing a centralized portal that users can use to submit inquiries, requests, or complaints related to their personal data through the official

[10] WA Dairobbi, 'Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam Layanan Transportasi Berbasis Aplikasi Online' (2020) <http://repository.uir.ac.id/id/eprint/9721>.

[11] Zhang Yiming, 'Tiktok Privacy Policy', *Tiktok.com* (2024) <https://www.tiktok.com/legal/page/row/privacy-policy/id>.

page https://www.tiktok.com/legal/report/privacy. Through this portal, users can submit various requests concerning their data rights in a structured and documented manner. If users are dissatisfied with the response or outcome of their submitted request, TikTok also provides an appeal mechanism that can be accessed by following the instructions provided in TikTok's official communications. Furthermore, TikTok implements supplementary terms tailored to the jurisdiction of each country, including information regarding local contacts or legal representatives, to ensure that user rights can be effectively enforced in accordance with the applicable local laws.

The clarity provided in TikTok's policy helps empower users to exercise meaningful control over their data. Notably, the right to access enables individuals to examine what personal data has been collected and how it is utilized. Users can request comprehensive disclosures about the categories, sources, and purposes of the data processing activities. Additionally, the right to rectification permits users to request updates or corrections to inaccurate or outdated information. This ensures that personal data held by the platform is accurate and up to date.

Among the most critical rights is the right to erasure, colloquially known as the "right to be forgotten." This entitles users to demand the deletion of their personal data, barring circumstances in which the platform has a compelling legal reason or legitimate interest to retain the data. By invoking this right, users can ensure that obsolete, irrelevant, or sensitive data is purged from the platform's records. The right to erasure is particularly important in the digital age, where outdated data can resurface and cause reputational harm or privacy infringements.[12]

According to legal scholar Philipus M. Hadjon, legal protection is categorized into preventive and repressive dimensions. In the domain of personal data regulation, repressive legal protection becomes especially pertinent when digital platforms, such as social media companies, fail to comply with established obligations, including the duty to delete user data upon request. Repressive protection, as Hadjon describes, focuses on dispute resolution and provides avenues for users to pursue compensation or sanctions after a violation has occurred. This principle is reflected in Indonesia's Law No. 27 of 2022 on Personal Data Protection (PDP Law), particularly Articles 57 and 58, which grant users the right to demand accountability through litigation or administrative measures in the event of non-compliance. Complementing Hadjon's view, Paul De Hert and Serge Gutwirth (2006) emphasize that legal frameworks must not only recognize individual rights but also include enforceable mechanisms to ensure those rights are upheld in practical terms, particularly in the digital context where asymmetries of power between platforms and users persist.

Daniel J. Solove adds a normative dimension by arguing that privacy violations are not limited to surveillance or unauthorized access but also include neglectful data retention and improper deletion practices, which can lead to long-term reputational and psychological harm. His theory supports the conceptualization of the "right to be forgotten" as more than symbolic—it is a crucial remedy to restore control over one's digital identity. Furthermore, Graham Greenleaf stresses that effective data protection requires a strong regulatory regime backed by independent oversight, transparency in enforcement, and harmonization with international standards such as the GDPR. These scholars collectively argue that mere consent mechanisms are insufficient in protecting

[12] Ibid.

users; rather, a robust framework grounded in repressive legal remedies is essential to ensure platforms respect user autonomy and the fundamental right to privacy. Therefore, the failure of social media platforms to uphold data deletion obligations, even when users have agreed to terms of service, may constitute a breach of personal data rights that justifies legal action under national and international data protection laws.

In conclusion, the protection of personal data in the context of social media is a multidimensional issue that intersects with international and domestic legal principles, individual rights, and corporate responsibilities. Legal instruments such as the GDPR, Indonesian PDP Law, and TikTok's internal policies collectively establish a framework within which personal data must be handled with transparency, accountability, and respect for individual autonomy. As digital platforms continue to grow in influence, the importance of robust personal data protection mechanisms will only become more pronounced. Upholding these principles is not merely a legal obligation but the cornerstone for fostering essential digital trust in a rapidly evolving technological landscape. When procedural gaps in legislation force users to navigate a labyrinth of inconsistent, platform-specific policies to exercise a fundamental right like data deletion, it erodes confidence in the entire digital ecosystem. This trust deficit can stifle innovation and engagement. Therefore, safeguarding user privacy effectively requires moving beyond the declaration of rights to the meticulous design of their execution. By mandating clear, standardized, and user-centric procedures for data control—inspired by rigorous comparative legal analysis—policymakers can transform privacy from a passive promise into an active, reliable guarantee. This ensures that corporate responsibilities are concretely defined and enforceable, ultimately creating a sustainable environment where technological advancement and individual autonomy are mutually reinforcing, rather than fundamentally at odds.[13]

3.2 Responsibility of Social Media Providers in Cases of Personal Data Breaches

In the context of personal data breaches on social media platforms, legal protection is generally categorized into preventive and repressive measures. As articulated by Philipus M. Hadjon, repressive legal protection refers to legal mechanisms that focus on resolving disputes after a violation has occurred. Within the framework of liability law, repressive protection involves juridical responses to conflicts that arise between platform operators and their users. These responses aim to provide remedies for harms already sustained, particularly due to negligence or misconduct in the management of users' personal data.[14]

In the Indonesian legal system, Law No. 27 of 2022 on Personal Data Protection provides clear guidance on repressive measures. Specifically, Article 57, paragraph 2 outlines several administrative sanctions that may be imposed on entities, including social media providers, that violate data protection obligations. These sanctions are designed

[13] Sinta Rosadi, 'Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia' (2018) 5(2) *Brawijaya Law Journal* 143.

[14] Wolfgang Kerber, 'Digital Markets , Data , and Privacy : Competition Law , Consumer Law , and Data Protection Joint Discussion Paper Series in Economics by the Universities of Wolfgang Kerber Digital Markets , Data , and Privacy : Competition Law , Consumer Law , and Data' (14).

to deter future misconduct and promote greater accountability among data controllers. The stipulated sanctions include:

a) Issuance of written warnings;

b) Temporary suspension of personal data processing activities;

c) Mandatory deletion or destruction of compromised personal data;

d) Imposition of administrative fines.

These measures are indicative of a legal system that seeks not only to punish but also to prevent recurrence by instilling a sense of responsibility in digital platform providers. The inclusion of administrative sanctions reinforces the need for social media companies to uphold data protection principles as mandated by law.

Furthermore, Law No. 27 of 2022 establishes the legal rights of individuals (data subjects) in relation to the automated processing of their personal data. Article 10, paragraph 1 of the law specifies that data subjects possess the right to object to decisions that are exclusively based on automated data processing. This provision aims to ensure that individuals are not subjected to potentially unjust or opaque algorithmic decision-making without the opportunity for human oversight or intervention.

In cases where the data controller fails to address such objections or if a violation has occurred, data subjects are entitled to pursue legal remedies. Article 12, paragraph 1 of the same law provides that individuals have the right to file lawsuits and claim compensation for any breach of their personal data rights. This provision offers a crucial avenue for redress and reinforces the legal accountability of data controllers, including social media platforms, when they mishandle or exploit user data without consent.[15]

According to Paterson and McDonagh, these statutory rights form a fundamental part of data protection governance, as they enable users to seek justice through institutional mechanisms. By embedding the right to compensation in the legal framework, the Indonesian law aligns with international standards that emphasize the empowerment of data subjects and the enforcement of digital rights. [16]

The legal responsibilities of social media platforms regarding personal data breaches encompass both preventive obligations and repressive consequences. On the preventive side, these platforms are mandated to adopt robust security measures—such as encryption, access controls, and regular audits—to minimize the risk of data leaks. This involves implementing technical and organizational safeguards that comply with data protection laws and international best practices. A proactive approach not only reduces the likelihood of breaches but also reinforces public trust in digital platforms.

---

[15] Moira Paterson and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* 1 <https://www.monash.edu/__data/assets/pdf_file/0009/1593630/Paterson-and-McDonagh.pdf>.

[16] Moira Paterson and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* 1 <https://www.monash.edu/__data/assets/pdf_file/0009/1593630/Paterson-and-McDonagh.pdf>.

From a repressive standpoint, platforms must be held accountable when their data processing activities result in user harm. This accountability includes providing restitution to affected users, complying with government-imposed penalties, and addressing regulatory investigations in a transparent manner. The dual nature of preventive and repressive frameworks illustrates the multi-layered responsibility that social media platforms must bear in an increasingly data-driven society.[17]

A clearly articulated legal framework, supported by strict enforcement mechanisms, is essential for ensuring that social media companies uphold their data protection obligations. As Soraja argues, such a framework plays a vital role in promoting digital accountability and maintaining public confidence in online platforms. The increasing incidence of data breaches, especially on popular platforms with millions of users, underscores the urgent need for comprehensive legal oversight and corporate transparency in managing personal data.

In conclusion, the issue of social media liability for data leakage is both complex and pressing. Legal instruments such as Law No. 27 of 2022 not only provide protection to users but also delineate the responsibilities and liabilities of digital platforms. The study reveals that the practical execution of personal data deletion on social media platforms is overwhelmingly contingent upon the specific, and often unilateral, terms and conditions set by the service providers themselves. This procedural dependency underscores the normative ambiguity within the current legal framework. Furthermore, it substantiates that in cases of personal data breaches arising from a platform's fault or negligence, social media providers bear a clear legal obligation to provide compensation, with monetary damages being a primary form of redress. These conclusions affirm that robust user protection is not self-executing through rights declaration alone. They demonstrate that embedding explicit, standardized procedural mandates into legislation is a necessary step to translate corporate responsibilities from abstract principles into actionable duties. By doing so, a more equitable and accountable digital environment can be established—one that respects individual privacy and ensures that platforms are legally bound to protect the personal information.[18]

4. Conclusion

The erasure of personal data on a website is contingent upon the contractual agreement established between the involved parties. In the context of social media platforms, such agreements are formalized through the terms and conditions that users must accept. Once users provide their consent by agreeing to these terms, they become legally bound by the stipulations contained therein. Regarding the liability of social media platforms for personal data breaches, they may be held responsible to provide financial compensation to affected users. This obligation stems from the user's legal right to data protection. Therefore, if it is established that the platform has unlawfully disclosed or

[17] Yahya Ziqra, Mahmul Siregar and Jelly Leviza, 'Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online' (2021) 2(2) *Iuris Studia: Jurnal Kajian Hukum* 330.

[18] Albert Siahaan, 'URGENSI PERLINDUNGAN DATA PRIBADI DI PLATFORM MARKETPLACE TERHADAP KEMAJUAN TEKNOLOGI (Urgency of Personal Data Protection on Marketplace Platforms Against Technological Advances)' (2022) 52(2) *Majalah Hukum Nasional* 210.

failed to safeguard personal data, the affected user has the legal standing to pursue a claim for damages against the platform.

References

Agusta, Hendrawan, 'Keamanan Dan Akses Data Pribadi Penerima Pinjaman Dalam Peer to Peer Lending Di Indonesia' (2021) 15(1) *Krtha Bhayangkara* 11

GOSNELL, CYMONE, 'The General Data Protection Regulation: American Compliance Overview and the Future of the American Business.' (2019) 15(1) *Journal of Business & Technology Law* 165 <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=142055261&site=ehost-live>

Muhammad Fajri Fernando, 'Perlindungan Hukum Terhadap Data Pribadi Konsumen Pada Perdagangan Elektronik' [2022] *Jurnal Universitas Muhammadiyah Palembang*

Paterson, Moira and Maeve McDonagh, 'Data Protection in an Era of Big Data: The Challenges Posed by Big Personal Data' (2018) 44(1) *Monash University Law Review* 1 <https://www.monash.edu/__data/assets/pdf_file/0009/1593630/Paterson-and-McDonagh.pdf>

Peter Mahmud Marzuki, *Penelitian Hukum Edisi Revisi* (Kencana, 2017)

Rosadi, Sinta, 'Protecting Privacy On Personal Data In Digital Economic Era : Legal Framework In Indonesia' (2018) 5(2) *Brawijaya Law Journal* 143

Siahaan, Albert, 'URGENSI PERLINDUNGAN DATA PRIBADI DI PLATFORM MARKETPLACE TERHADAP KEMAJUAN TEKNOLOGI (Urgency of Personal Data Protection on Marketplace Platforms Against Technological Advances)' (2022) 52(2) *Majalah Hukum Nasional* 210

Soraja, Alga, 'Perlindungan Hukum Atas Hak Privasi Dan Data Pribadi Dalam Prespektif HAM' [2021] *Prosiding Seminar Nasional Kota Ramah Hak Asasi Manusia* 20

Syed Khurrum Hussain Naqvi, Komal Batool, 'A Comparative Analysis between General Data Protection Regulations and California Consumer Privacy Act' (2023) 4(1) *Journal of Computer Science, Information Technology and Telecommunication Engineering* 326

Wolfgang Kerber, 'Digital Markets , Data , and Privacy : Competition Law , Consumer Law , and Data Protection Joint Discussion Paper Series in Economics by the Universities of Wolfgang Kerber Digital Markets , Data , and Privacy : Competition Law , Consumer Law , and Data' (14)

Ziqra, Yahya, Mahmul Siregar and Jelly Leviza, 'Analisis Hukum General Data Protection Regulation (GDPR) Terhadap Data Pribadi Konsumen Dalam Melakukan Transaksi Online' (2021) 2(2) *Iuris Studia: Jurnal Kajian Hukum* 330

Dairobbi, WA, 'Perlindungan Hukum Terhadap Penyalahgunaan Data Pribadi Dalam Layanan Transportasi Berbasis Aplikasi Online' (2020) <http://repository.uir.ac.id/id/eprint/9721>

Muhammad Fajri Fernando, 'Perlindungan Hukum Terhadap Data Pribadi Konsumen Pada Perdagangan Elektronik (E-Commerce)' (2016)

Ramadha, Bagus Satryo, 'Kemampuan Hukum Pidana Terhadap Kejahatan Siber Terkait Perindungan Data Pribadi Di Indonesia' (Universitas Islam Indonesia, 2021) <chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.uii.ac.id/bitstream/handle/123456789/31626/18912046 Bagus Satryo Ramadha.pdf?sequence=1&isAllowed=y>

Zhang Yiming, 'Tiktok Privacy Policy', *Tiktok.com* (2024) <https://www.tiktok.com/legal/page/row/privacy-policy/id>

Law and Regulation

Law No. 27 of 2022 concerning Personal Data Protection, State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6802