International Journal of Social and Education (INJOSEDU) https://languar.net/index.php/INJOSEDU
Vol. 3 No. 1 April 2026, hal., 125-138 e-ISSN: 3047-6151

THE LEGAL IMPLICATIONS OF PERSONAL DATA PROTECTION FOR ELECTRONIC CONTRACTS FROM THE PERSPECTIVE OF INDONESIAN CIVIL LAW

Gunawan Widjaja
Senior Lecturer, Faculty of Law Universitas 17 Agustus 1945 Jakarta
widjaja_gunawan@yahoo.com

Abstract

The rapid growth of electronic transactions in Indonesia has made the protection of personal data a central issue in civil law, particularly regarding the validity and enforcement of electronic contracts. This study aims to analyse the legal implications of personal data protection on electronic contracts from the perspective of Indonesian civil law, focusing on how Law No. 27 of 2022 on Personal Data Protection (PDP Law) affects the validity requirements of contracts and the civil liabilities of the parties. The research method employed is normative legal research using a literature review approach, analysing primary legal sources such as the Civil Code, the ITE Law, and the PDP Law, as well as relevant secondary and tertiary legal materials. The research findings indicate that the PPDL has brought about a fundamental transformation in the legal framework of electronic contracts, wherein the consent of data subjects must meet the standards of *informed consent*—being explicit, specific, informative, and voluntary—to ensure that the element of agreement under Article 1320 of the Civil Code is materially fulfilled. Violations of personal data protection provisions may be classified as breach of contract or unlawful acts giving rise to civil liability in the form of damages, with a reversal of the burden of proof mechanism that places the data subject in a stronger position. It is concluded that the harmonisation between the Civil Code, the ITE Law, and the PDP Law has created a more comprehensive civil legal ecosystem, although the effectiveness of its enforcement still requires the strengthening of digital legal literacy and consistency in court jurisprudence.

Keywords: personal data protection, electronic contracts, civil law, the Personal Data Protection Act, *informed consent*, civil liability, breach of contract.

Introduction

Developments in information and communication technology have fundamentally transformed the landscape of social, economic and legal interactions in Indonesia, particularly in the practice of electronic transactions, which have now become the backbone of digital commerce. This digital transformation has not only accelerated business processes but has also created new complexities in legal relationships between parties, particularly regarding the management of personal data, which is a crucial element in every electronic contract (Misdarti, 2025) .

Personal data has become a high-value commodity within the digital economy ecosystem, where every electronic transaction requires the collection, storage and processing of users' personal information for the purposes of verification,

authentication and service personalisation. However, the increase in the volume of electronic transactions, which reached Rp262.08 trillion in the third quarter of 2025, has not been matched by adequate legal awareness regarding the protection of personal data, thereby creating vulnerabilities to data misuse and breaches (Indonesian Payment Systems Association [ASPI], 2025).

The phenomenon of personal data breaches in Indonesia shows an alarming trend, with the number of cases more than tripling from 35 in 2023 to 111 in 2024, placing Indonesia among the top 10 countries with the highest incidence of data breaches worldwide (Rinjani & Firmansyah, 2025) . This situation indicates structural weaknesses in personal data protection mechanisms, particularly in the context of electronic agreements which often disregard the principles of transparency and accountability in user consent clauses.

In response to this urgency, the Indonesian Government enacted Law No. 27 of 2022 on Personal Data Protection (PDP Law), which marks a historic milestone in strengthening the legal framework for personal data protection as part of human rights and individual civil rights (Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection, 2022). This regulation not only sets out the obligations of data controllers and processors, but also grants substantive rights to data subjects to control their personal information.

From a civil law perspective, personal data constitutes an object of civil rights inherent to the individual; consequently, any breach of personal data may be classified as a tortious act as provided for in Article 1365 of the Civil Code (KUHPerdata) (Yudha et al., 2025) . The legal consequences of such breaches include liability for compensation for both material and non-material losses suffered by the data subject as a result of the leakage or misuse of their personal data.

Electronic agreements, as the primary legal instrument in digital transactions, must fulfil the requirements for a valid agreement as set out in Article 1320 of the Civil Code, namely: mutual consent, legal capacity, a specific subject matter, and a lawful cause; these requirements are now reinforced by the provisions of Law No. 11 of 2008 on Information and Electronic Transactions, as amended by LawNo. 19 of 2016 (ITE Law) (Oktaviana & Lumbantobing, 2026). However, the validity of an electronic contract does not depend solely on procedural formalities, but also on the substance of the consent given by the user regarding the management of their personal data.

The principle of agreement in electronic contracts becomes problematic when user consent is obtained through ‘click-wrap’ or ‘browse-wrap’ mechanisms, which often fail to provide an adequate understanding of the legal implications of the privacy clauses to which consent is given. In this context, the principles of transparency and informed consent, as mandated by the Personal Data Protection Act, constitute substantive prerequisites for the validity of electronic contracts; for without materially valid consent, the contract may be void ab initio or voidable (Septiari & Ujianti, 2025) .

The legal implications of personal data protection for electronic contracts are also evident in the area of civil liability, where data controllers who breach the provisions of the Personal Data Protection Act may face administrative, civil, or even criminal sanctions, depending on the severity of the breach and the resulting harm (Yudha et al., 2025) . This civil liability includes the obligation to compensate data subjects for the losses they have suffered, which may take the form of direct financial losses or non-material losses such as the loss of privacy and reputation.

Major data breaches such as the Dukcapil data breach, the Bank Syariah Indonesia customer data breach, and the NPWP data breach—which affected millions of citizens in 2023–2024—highlight weaknesses in the implementation of data security principles as required by the Personal Data Protection Act (PDP Act). These cases not only harm individuals as data subjects, but also undermine public trust in the electronic transaction ecosystem and hinder the growth of the national digital economy.

From a civil law perspective, the legal relationship between the data controller and the data subject in an electronic contract can be characterised as a contractual relationship giving rise to reciprocal rights and obligations, whereby the data controller is obliged to protect personal data as part of the performance of the contract (Truli, 2018) . A breach of this obligation constitutes a breach of contract or an unlawful act, entitling the data subject to claim performance, rescission of the contract, or damages.

However, the effectiveness of civil law protection for personal data in electronic contracts still faces significant challenges, including low levels of digital legal literacy among the public, weak enforcement mechanisms, and the absence of consistent case law to guide the courts in resolving personal data protection disputes (Supeno et al., 2025) . This situation requires harmonisation between the provisions of the Civil Code, the ITE Law, and the PDP Law to create comprehensive legal certainty.

Based on the above, this article aims to analyse the legal implications of personal data protection for the validity and enforcement of electronic contracts from the perspective of Indonesian civil law, focusing on two main areas: firstly, the legal framework for personal data protection under the Personal Data Protection Act (PDP Act) and its relationship with civil rights; and secondly, the implications of personal data protection breaches for the validity, enforcement, and liability in electronic contracts. It is hoped that this analysis will provide an academic and practical contribution to the strengthening of the Indonesian civil law system in the digital economy era.

Research Methodology

This study employs a normative legal research method using *a* literature review approach, focusing on the analysis of primary, secondary and tertiary legal sources to examine the legal implications of the Personal Data Protection Act on electronic contracts from the perspective of Indonesian civil law. Primary legal sources include the Civil Code (KUHPerdata), Law No. 11 of 2008 on Electronic Information and Transactions,

as amended by Law No. 19 of 2016, and Law No. 27 of 2022 on Personal Data Protection, which form the primary normative basis for this analysis. Secondary legal materials include books, national and international journal articles, and previous research relevant to personal data protection, electronic contracts, and civil liability, whilst tertiary legal materials consist of legal dictionaries, encyclopaedias, and reliable online sources used to clarify key concepts (Eliyah & Aslan, 2025) . Data collection was carried out through a documentary study by examining, classifying, and systematising these legal materials, which were then analysed qualitatively using grammatical, systematic, and teleological interpretation methods to construct a coherent and comprehensive legal argument regarding the status of personal data as an object of civil rights and the implications of its infringement on the validity and implementation of electronic contracts (McConville, 2017) .

Results and Discussion

Personal Data Protection within the Indonesian Legal Framework

The protection of personal data in Indonesia has undergone a fundamental transformation with the enactment ofNo. 27 of 2022 on Personal Data Protection (PDP Law), which serves as the first comprehensive legal framework specifically regulating individuals' rights over their personal data and the obligations of parties processing such data (Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection, 2022). Prior to the PDP Act, personal data protection provisions were scattered across various sectoral regulations that were fragmented and failed to provide adequate protection, leading to Indonesia being regarded as lagging behind other ASEAN countries that already had similar regulations (Supeno et al., 2025) .

The Personal Data Protection Act defines personal data as data relating to an identified or identifiable natural person, either on its own or in combination with other information, whether directly or indirectly, through electronic or non-electronic systems, encompassing both general personal data and specific personal data (Article 1(1) of the Personal Data Protection Act). General personal data includes full name, gender, nationality, religion, and combined data used to identify an individual, whilst specific personal data includes health data, biometric data, genetic data, data concerning sexual life, political views, criminal records, and data on children requiring a higher level of protection (Article 4 of the PDP Act).

The philosophical basis for the protection of personal data in the Personal Data Protection Act stems from the recognition that the protection of personal data is part of the human rights guaranteed by the 1945 Constitution of the Republic of Indonesia, specifically Article 28G(1), which guarantees the right to protection of one's person, family, honour, dignity, and property, as well as the right to a sense of security and protection from the threat of fear of doing or not doing something that constitutes a human right (Yudha et al., 2025) . This recognition positions personal data not merely as

an economic object, but as an extension of an individual's personality to which civil rights are attached that must be respected and protected.

The Personal Data Protection Act (PDP Act) sets out six fundamental principles that must be adhered to by every data controller and data processor when processing personal data, namely the principles of transparency, purpose limitation, data minimisation, accuracy, storage limitation, and security and confidentiality (Versaci, 2018) . The principle of transparency requires the data controller to provide clear, honest, and easily understandable information to the data subject regarding the identity of the controller, the purpose of the processing, the type of data collected, and the rights of the data subject before processing takes place.

The principle of purpose limitation requires that personal data be processed only for specific, explicit and legitimate purposes, and must not be further processed in a manner incompatible with the original purpose without the data subject's additional consent (Supeno et al., 2025) . The principle of data minimisation restricts the collection of personal data to only the types and amounts of data that are relevant and limited to what is necessary to achieve the processing purposes, thereby preventing the practice of excessive data collection that frequently occurs in electronic transactions.

The principle of accuracy requires data controllers to ensure that personal data being processed is accurate, complete, not misleading, and up to date in accordance with the purposes of processing, and to provide mechanisms for data subjects to correct, update, or delete inaccurate data (Agusta, 2022). The principle of storage limitation requires that personal data be stored only for as long as is necessary to achieve the purposes of processing, after which it must be erased or destroyed unless there is another legal obligation requiring longer storage. The principles of security and confidentiality require data controllers and processors to implement adequate technical and organisational measures to protect personal data from unauthorised access, leakage, misuse, or damage.

The Personal Data Protection Act also sets out in detail the rights of data subjects, comprising nine substantive rights, namely the right to obtain information regarding the identity of the data controller, the legal basis for the processing, the purpose of the request and the use of personal data, as well as the accountability of the party requesting the personal data (Section 5 of the Personal Data Protection Act); the right to supplement, update, and/or correct errors and/or inaccuracies in personal data concerning oneself in accordance with the purpose of personal data processing (Article 6 of the Personal Data Protection Act; the right to access and obtain a copy of personal data concerning them in accordance with the provisions of laws and regulations (Article 7 of the PDP Act); the right to cease processing, delete, and/or destroy their personal data in accordance with the provisions of laws and regulations (Article 8 of the PDP Act); the right to withdraw consent previously given for the processing of their personal data (Article 9 of the PDP Act); the right to object to decisions based on automated

processing, including profiling (Article 10 of the PDP Act); the right to suspend or restrict the processing of personal data in a proportionate manner in accordance with the purpose of the processing (Article 11 of the PDP Act); the right to bring a claim and receive compensation for breaches of the processing of their personal data in accordance with the provisions of the law (Section 12 of the PDP Act); and the right to receive personal data concerning themselves or to consent to the transfer of their personal data to another data controller in a structured and commonly used format (Article 13 of the PDP Act) (Sylviana et al., 2025) .

Within the institutional framework of the Personal Data Protection Act (PDP Act), there are two key actors with legal responsibilities: the data controller and the data processor. The data controller is the party that determines the purposes of and exercises control over the processing of personal data, whilst the data processor is the party that processes personal data on behalf of the data controller (Rinjani & Firmansyah, 2025) . The data controller bears primary responsibility for compliance with the Personal Data Protection Act (PDP Act), including the obligation to appoint a Data Protection Officer (DPO) where data processing is carried out for the purposes of public service, where processing requires regular monitoring and evaluation of personal data on a large scale, or where the processing of specific personal data and/or personal data on a large scale has the potential to pose a high risk to the rights of data subjects (Article 53 of the PDP Act) (Rinjani & Firmansyah, 2025) .

The obligations of data controllers and processors under the Personal Data Protection Act include the obligation to obtain valid consent from the data subject prior to processing personal data, unless there is another valid legal basis such as the performance of a contract, a legal obligation, the vital interests of the data subject, the public interest, or the performance of the duties of a public authority (Article 20 of the PDP Act) (Yu & Zhao, 2019) . Consent must be given in writing or through a verifiable record, of one's own free will (voluntary), specific, informed, and unambiguous, and may be withdrawn at any time by the data subject without causing them any detriment. The data controller is also obliged to carry out a Data Protection Impact Assessment (DPIA) if the processing of data has the potential to pose a high risk to the rights of the data subject, such as the large-scale processing of sensitive data or the use of new technologies that are invasive of privacy (Rinjani & Firmansyah, 2025) .

The PDP Act also imposes strict prohibitions on unlawful acts relating to personal data, whereby no person shall unlawfully obtain or collect personal data that does not belong to them with the intention of benefiting themselves or others, which may result in harm to the data subject (Section 65(1) of the PDP Act) (Ventura & Coeli, 2018) . The prohibition also applies to the disclosure of personal data not belonging to the individual, the misuse of personal data, and the falsification of personal data with the intention of benefiting oneself or others, which may result in harm to the data subject,

carrying a maximum prison sentence of 5 to 6 years and a maximum fine of Rp5 billion to Rp6 billion (Sections 65–67 of the Personal Data Protection Act).

From a law enforcement perspective, the Personal Data Protection Act (PDP Act) sets out three types of sanctions that may be imposed on offenders, namely administrative sanctions, civil sanctions and criminal sanctions (Versaci, 2018) . Administrative sanctions are imposed by the competent personal data protection authority and may take the form of a written warning, a temporary suspension of personal data processing activities, the deletion or destruction of personal data, and/or an administrative fine of up to 2% of the annual revenue or annual income of the offender (Article 57 of the PDP Act) (Putri & Putra, 2024) . Civil sanctions take the form of compensation that may be claimed by data subjects who have suffered loss as a result of a personal data processing breach; such loss may be material or immaterial, and may be resolved through the courts or alternative dispute resolution mechanisms outside the courts.

Civil liability under the Personal Data Protection Act (PDP Act) adopts the principle of strict liability under certain conditions, whereby data controllers may be held liable without the need to prove fault; it is sufficient to prove the existence of damage and a causal link between the breach and the damage suffered (Truli, 2018) . This mechanism provides stronger protection for data subjects, given the imbalance in bargaining power and access to information between individuals and data-controlling corporations, as well as the difficulties in proving liability often faced by victims of data breaches under conventional legal systems.

The implementation of the Personal Data Protection Act (PDP Act) since October 2024 has faced significant challenges, including low legal awareness among businesses, limited resources within supervisory bodies, the complexity of data processing technology, and the lack of consistent case law to guide law enforcement (Piansah, 2024) . However, the existence of the Personal Data Protection Act has created a new paradigm in civil law relations in the digital age, where personal data is no longer viewed as a free commodity that can be exploited without limit, but rather as a civil right inherent to the individual and protected by law, with serious consequences for violators.

Overall, Indonesia's legal framework for personal data protection under the Personal Data Protection Act (PDP Act) has adopted international standards that are in line with the European Union's General Data Protection Regulation (GDPR) and similar regulations in other developed nations, thereby not only strengthening the protection of individual rights but also enhancing public trust and the competitiveness of Indonesia's digital economy on the global stage. A thorough understanding of this legal framework is an essential prerequisite for every party involved in electronic transactions to ensure legal compliance and avoid the risk of civil liability that may arise from breaches of personal data protection provisions.

Implications of Personal Data Protection on the Validity and Enforcement of Electronic Agreements

Electronic agreements, as the primary legal instrument in digital transactions in Indonesia, must satisfy the requirements for the validity of an agreement as set out in Article 1320 of the Civil Code (KUHPerdata), namely: the consent of the parties, the capacity to enter into a contract, a specific subject matter, and a lawful cause, which is now reinforced by the provisions of Article 18(1) of Law No. 11 of 2008 on Information and Electronic Transactions, as amended by Law No. 19 of 2016 (ITE Law)(Oktaviana & Lumbantobing, 2026) . The introduction of the Personal Data Protection Act (PDP Act) adds a new dimension to these validity requirements, whereby the consent given by the data subject in an electronic agreement must not only fulfil the elements of a formal agreement, but must also constitute consent that is materially valid in accordance with the standards of the PDP Act, namely explicit, specific, informative, and freely given (Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection, 2022).

The principle of consent as the primary condition for the validity of a contract has undergone a significant transformation in the context of electronic contracts involving the processing of personal data, where consent can no longer be obtained through implicit mechanisms or silent consent(silent consent), but must take the form of an explicit and active statement by the data subject, documented in writing or recorded (Sylviana et al., 2025). Consent given implicitly (implied consent) through passive actions such as continuing to browse a website or failing to tick the opt-out option in an online form no longer meets the standard of informed consent required by the Personal Data Protection Act, meaning that electronic agreements built upon such consent may be deemed to be vitiated by lack of free will and potentially void ab initio or subject to annulment (Sylviana et al., 2025) .

The legal implications of the Personal Data Protection Act (PDP Act) regarding the element of consent in electronic agreements are also evident in the data controller's obligation to provide clear, comprehensive and easily understandable information to the data subject before consent is given, including the identity of the data controller, the purpose of processing, the type of data collected, the retention period, the data subject's rights, and the legal consequences should consent not be given (Article 20(2) of the PDP Act) (Yudha et al., 2025) . The absence or incompleteness of this information results in the consent being defective (defective consent), which from a civil law perspective may be classified as mistake (dwaling) or fraud (bedrog) that nullifies the agreement as provided for in Article 1321 of the Civil Code.

In the practice of electronic contracts in Indonesia, the consent mechanism is often implemented through standard clauses or standard contracts drafted unilaterally by electronic system operators and presented in the form of 'click-wrap agreements' or 'browse-wrap agreements', which users must accept without room for negotiation

(Kuspraningrum, 2011) . Although standard clauses are permitted provided they do not violate the principle of freedom of contract and the provisions ofNo. 8 of 1999 on Consumer Protection, the Personal Data Protection Act imposes substantive restrictions by prohibiting clauses that are exploitative, non-transparent, or disregard the rights of data subjects; consequently, privacy clauses that are overly broad, ambiguous, or grant unlimited authority to the data controller may be declared null and void (Susanty et al., 2022) .

The element of legal capacity in electronic contracts also takes on a new dimension in the context of the Personal Data Protection Act, under which the processing of personal data of minors requires specific consent from a parent or legal guardian, in accordance with the provisions of Article 21 of the PDP Act, which prohibits the processing of a child's personal data without the explicit consent of the holder of parental authority (Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection, 2022). An electronic agreement involving the collection of a child's data without meeting these requirements not only breaches the Personal Data Protection Act but may also be deemed to lack the element of legal capacity under Article 1320 of the Civil Code, thereby rendering the agreement voidable upon a claim by the child's parent or legal guardian.

Certain aspects of the subject matter in the conditions for the validity of a contract are also affected by the Personal Data Protection Act, whereby personal data that forms the subject matter of processing in an electronic contract must be defined specifically and limited to what is necessary to achieve the purpose of the contract (the principle of data minimisation), so that excessive data collection or collection beyond the agreed purpose may be classified as a breach of the requirement for a specific subject matter of the contract (Supeno et al., 2025) . In civil disputes, data subjects may bring a claim on the grounds that the subject matter of the agreement has become indeterminate or exceeds the agreed limits as a result of data collection practices that do not comply with the data minimisation principle under the Personal Data Protection Act.

The lawful purpose as the fourth condition for the validity of a contract has been reaffirmed by the Personal Data Protection Act (PDPA), whereby the purpose of processing personal data must be lawful, not contrary to legislation, public order, morality, or the public interest (Section 20 of the PDPA) (Yu & Zhao, 2019) . Electronic agreements intended to process personal data for unlawful purposes, such as fraud, discrimination, market manipulation, or other criminal activities, are not only null and void under Article 1335 of the Civil Code, but may also give rise to criminal liability for the parties involved in accordance with the provisions of the Personal Data Protection Act.

The implications of personal data protection for the performance of electronic contracts are evident in the data controller's obligation to fulfil their contractual obligations in accordance with the principles of data security and confidentiality as

required by the Personal Data Protection Act (PDP Act), whereby failure to protect personal data from leaks, unauthorised access, or misuse may be classified as a breach of contract (default) under civil law (Septiari & Ujianti, 2025) . Such a breach may take the form of a complete failure to perform, performing the obligation late, performing the obligation improperly, or doing something that the contract prohibits; all of which entitle the data subject to claim performance, rescission of the contract, or damages in accordance with Article 1243 of the Civil Code.

In the context of civil liability, a breach of personal data protection provisions in the performance of an electronic contract may give rise to two types of legal claims: claims based on breach of contract and claims based on tort (onrechtmatige daad) in accordance with Article 1365 of the Civil Code (Truli, 2018) . A claim for breach of contract is brought where there is a breach of a contractual obligation explicitly or implicitly set out in the electronic agreement, whilst a claim for tort may be brought even in the absence of a direct contractual relationship, provided that a breach of the data subject's subjective rights, the data controller's legal obligations, public policy, or reasonable care can be established.

The large-scale data breaches that occurred in Indonesia in 2023–2024, such as the Bank Syariah Indonesia customer data breach involving 15 million customers and the Tokopedia e-commerce data breach-commerce platform Tokopedia affecting 91 million users, demonstrate how a data controller's failure to fulfil its data protection obligations may be classified as a breach of contract and an unlawful act, thereby entitling data subjects to claim compensation for both material and immaterial damages (Nugroho et al., 2024) . In such disputes, data subjects may bring a claim based on the actual losses suffered, such as financial losses resulting from fraud exploiting leaked data, risk mitigation costs (card replacement, credit monitoring), and non-material losses in the form of loss of privacy, psychological distress, and reputational damage.

The Personal Data Protection Act (PDP Act) also introduces a mechanism for the reversal of the burden of proof in civil disputes concerning the protection of personal data, whereby the data controller being sued is required to prove that it has fulfilled its data protection obligations in accordance with the standards of the PDP Act, rather than the data subject having to prove the data controller's negligence (Section 12 of the PDP Act) (Putri & Putra, 2024) . This mechanism gives the data subject a stronger position in litigation, given the imbalance in access to information and technical capacity between individuals and corporate data controllers, as well as the inherent difficulty in proving technical negligence within complex data processing systems.

Civil sanctions under the PDP Act include the obligation to compensate data subjects for losses suffered, which may be resolved through the district court or alternative dispute resolution mechanisms outside the courts, such as mediation, arbitration or conciliation, in accordance with the provisions of the law (Section 58 of the PDP Act) (Ventura & Coeli, 2018) . The amount of compensation is determined by

the court based on proven actual losses, which may include direct losses (actual loss), future losses (lost profit), mitigation costs, and even non-pecuniary damages assessed on a reasonable basis, taking into account the severity of the breach, the number of victims, and the resulting social impact.

In addition to individual liability, the PDP Act also recognises joint and several liability between data controllers and data processors where a breach occurs due to the fault of both parties, thereby enabling data subjects to claim compensation from either or both parties simultaneously (Section 59 of the PDP Act)(Supeno et al., 2025) . This provision provides stronger protection for data subjects by broadening the basis for claiming compensation, whilst creating an incentive for data controllers and data processors to monitor one another and ensure compliance with data protection standards throughout the entire processing chain.

Overall, the implications of the Personal Data Protection Act (PDP Act) for the validity and enforcement of electronic contracts under Indonesian civil law create a new paradigm in which the protection of personal data is no longer merely a sectoral regulatory obligation, but rather a substantive element that determines the validity of contracts and gives rise to civil liability for violators. Harmonisation between the Civil Code, the ITE Law, the PDP Law, and the Consumer Protection Law is an essential prerequisite for creating legal certainty for businesses and effective protection for data subjects within Indonesia's rapidly evolving electronic transaction ecosystem.

Conclusion

The protection of personal data within the Indonesian legal framework, as set out in Law No. 27 of 2022 on Personal Data Protection (PDP Law), has brought about a fundamental transformation in the structure of civil law, whereby personal data is no longer viewed merely as an economic commodity, but rather as a civil right inherent to the individual and protected as part of human rights. The legal principles of personal data protection, which encompass transparency, purpose limitation, data minimisation, accuracy, storage limitation, as well as security and confidentiality, have become binding normative standards for every data controller and processor in fulfilling their contractual obligations, such that breaches of these principles not only result in administrative and criminal sanctions, but also civil liability in the form of compensation for both material and non-material losses suffered by the data subject.

The legal implications of personal data protection for electronic contracts from the perspective of Indonesian civil law are evident in the four conditions for the validity of a contract as set out in Article 1320 of the Civil Code, whereby the consent given by the data subject must meet the standards of informed consent—which must be explicit, specific, informative, and voluntary in accordance with the Personal Data Protection Act so that the element of agreement is fulfilled in substance, not merely as a procedural formality. Failure to meet these consent standards results in an electronic contract

being vitiated by a defect of consent and subject to annulment, whilst a breach of data protection obligations in the performance of the agreement may be classified as a breach of contract or an unlawful act, giving rise to the data subject's right to claim performance, rescission of the agreement, or damages through a mechanism of reversal of the burden of proof that places the victim of the breach in a stronger position.

Overall, the harmonisation of the Civil Code, the Electronic Information and Transactions Act, and the Personal Data Protection Act has created a more comprehensive civil law ecosystem that is adaptable to the dynamics of electronic transactions in the digital age, where personal data protection is a determining factor for the validity and enforcement of electronic contracts. However, the effectiveness of this civil law enforcement still requires strengthening through improved public digital legal literacy, consistent court jurisprudence, and the institutional capacity of supervisory bodies, so that the civil rights of data subjects can be optimally protected without hindering innovation and the sustainable growth of Indonesia's digital economy.

References

Agusta, H. (2022). Telaah Yuridis Aplikasi Zoom Dalam Mengumpulkan Data Pribadi Ditinjau Dari Peraturan Pemerintah No. 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik. *KRTHA BHAYANGKARA*, *16*(1). https://doi.org/10.31599/krtha.v16i1.1204

Eliyah, E., & Aslan, A. (2025). STAKE'S EVALUATION MODEL: METODE PENELITIAN. *Prosiding Seminar Nasional Indonesia*, *3*(2), Article 2.

Kuspraningrum, E. (2011). Keabsahan Kontrak Elektronik Dalam UU ITE Ditinjau Dari Pasal 1320 KUHPerdata dan UNCITRAL Model Law On Electronic Commerce. *Risalah Hukum*, 64–76.

McConville, M. (2017). *Research Methods for Law*. Edinburgh University Press.

Misdarti, M. (2025). *Pengaruh E-Commerce, E-Money, Pinjaman Online, Impor Barang Konsumsi, Inflasi dan Suku Bunga terhadap Pengeluaran Konsumsi Rumah Tangga di Indonesia* [Other, Universitas Jambi]. https://doi.org/10/8/FULL_SKRIPSI_MISDARTI_C1A020027.pdf

Nugroho, F. N. P., Listanto, M. F., Amelia, N., & Annisa, S. (2024). Analisis Kebocoran Data Pribadi Dalam Media Sosial. *Fibonacci: Jurnal Ilmu Ekonomi, Manajemen Dan Keuangan*, *1*(2), 58–65. https://doi.org/10.63217/fibonacci.v1i2.70

Oktaviana, S., & Lumbantobing, T. (2026). *HUKUM PERANCANGAN KONTRAK: (TEORI, PRAKTIK DAN PERKEMBANGAN DI ERA DIGITAL)*. Dunia Penerbitan buku.

Piansah, A. (2024). The Role of Civil Law in Realizing Personal Data Security in the Era of Digital Transformation in Indonesia. *Zona Law And Public Administration Indonesia*, *2*(4), 13–22.

Putri, T. S., & Putra, M. R. S. (2024). Implementasi Undang-Undang Pelindungan Data Pribadi: Peran Manajemen Risiko Hukum bagi Prosesor Data Pribadi. *Jurnal*

Hukum Lex Generalis, *5*(4). https://ojs.rewangrencang.com/index.php/JHLG/article/view/730

Rinjani, M. A., & Firmansyah, R. (2025). Hambatan Implementasi UU 27/2022 dan Strategi Penguatan Perlindungan Data Pribadi di Indonesia. *Jurnal Analisis Hukum*, *8*(1), 70–83. https://doi.org/10.38043/jah.v8i1.6793

Septiari, N., & Ujianti, N. M. P. (2025). Kekuatan hukum perjanjian elektronik dalam perspektif KUH Perdata dan UU ITE. *Indonesian Journal of Law and Justice*, *2*(4), 10–10.

Supeno, S., Rosmidah, R., & Iqbal, S. M. U. (2025). Personal Data Protection in Review of Legal Theories and Principles. *Journal of Law and Legal Reform*, *6*(3), 1349–1376. https://doi.org/10.15294/jllr.v6i3.10252

Susanty, A. P., Rachmat, D., & Suhendro. (2022). PENCATUMAN KLAUSULA BAKU DALAM PERJANJIAN ONLINE PADA MEDIA SOSIAL BERDASARKAN ASAS KEBEBASAN BERKONTRAK. *Jotika Research in Business Law*, *1*(2), 68–81. https://doi.org/10.56445/jrbl.v1i2.46

Sylviana, G., Maharani, D. P., & Wibowo, A. M. (2025). Keabsahan Praktik Dark Patterns Terhadap Pemerolehan Persetujuan Pemrosesan Data Pribadi di Indonesia. *RechtJiva*. https://www.researchgate.net/profile/Afrizal-Wibowo/publication/392514975_Keabsahan_Praktik_Dark_Patterns_Terhadap_Pemerolehan_Persetujuan_Pemrosesan_Data_Pribadi_di_Indonesia/links/6846645fd1054b0207fab3bd/Keabsahan-Praktik-Dark-Patterns-Terhadap-Pemerolehan-Persetujuan-Pemrosesan-Data-Pribadi-di-Indonesia.pdf

Truli, E. (2018). The General Data Protection Regulation and Civil Liability. In M. Bakhoum, B. Conde Gallego, M.-O. Mackenrodt, & G. Surblytė-Namavičienė (Eds.), *Personal Data in Competition, Consumer Protection and Intellectual Property Law: Towards a Holistic Approach?* (pp. 303–329). Springer. https://doi.org/10.1007/978-3-662-57646-5_12

Ventura, M., & Coeli, C. M. (2018). Beyond privacy: The right to health information, personal data protection, and governance. *Cadernos de Saúde Pública*, *34*, e00106818. https://doi.org/https://doi.org/10.1590/0102-311X00106818

Versaci, G. (2018). Personal Data and Contract Law: Challenges and Concerns about the Economic Exploitation of the Right to Data Protection. *European Review of Contract Law*, *14*(4), 374–392. https://doi.org/10.1515/ercl-2018-1022

Yu, X., & Zhao, Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, *35*(5), 105318. https://doi.org/10.1016/j.clsr.2019.04.001

Yudha, Sahril, I., & Atmadja3, D. A. R. W. (2025). Perlindungan Data Pribadi Konsumen, Dokumen dan Tanda Tangan Elektronik yang Dipergunakan oleh Pihak Ketiga dalam Transaksi E-Commerce. *CENDEKIA : Jurnal Penelitian Dan Pengkajian Ilmiah*, *2*(2), 173–189. https://doi.org/10.62335/cendekia.v2i2.897

Asosiasi Sistem Pembayaran Indonesia. (2025). *Berita statistik sistem pembayaran Indonesia kuartal III 2025*. https://databoks.katadata.co.id

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 197.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 197.