Indonesian Journal of Advocacy and Legal Services
Vol. 8 Issue 1 (2026) 211-270
DOI: https://doi.org/10.15294/ijals.v8i1.37509
Available online since: June 8, 2026

Indonesian Journal of Advocacy & Legal Services
https://journal.unnes.ac.id/journals/ijals/index

The Consent Paradox: Evaluating the Validity of Sensitive Data Collection by AI Chatbots

Marianne Charleen Sabini [1]✉, Fajar Sugianto [1], Kentarou Kaneda [2], Vincensia EP Sari [1], Jerry Shalmont [1]

[1] Faculty of Law, Universitas Pelita Harapan, Tangerang, Indonesia
[2] Ginzaseiwa Law Office, Tokyo, Japan

✉ Corresponding email: *fajar.sugianto@uph.edu*

Abstract

This paper explores the legal friction between user consent and data collection practices, investigating whether the current Indonesian legal landscape provides sufficient safeguards for AI chatbot users. It employs a comparative legal analysis to evaluate the regulatory alignment between the Indonesian PDP Law and the EU GDPR, specifically regarding the protection of sensitive data. The analysis reveals that while the two regulations share foundational data protection principles, the PDP Law lacks necessary specificity regarding the definition and processing of sensitive data, risk assessment mechanisms, and the authority of supervisory bodies. The first analysis elucidates how these regulatory gaps hinder the PDP Law's ability to effectively govern AI-based environments and establish accountability for data controllers and processors. Subsequently, the second analysis proposes necessary reforms, including more robust governance mechanisms, strengthened

administrative oversight, and industry-specific guidelines to ensure uniform enforcement. This paper concludes that the PDP Law requires substantive refinement to remain effective and responsive to the rapid evolution of AI and automated systems.

Keywords *Sensitive Data Collection, AI Chatbots, Automated Processing, Personal Data Protection*

A. Introduction

By 2024, ChatGPT has over 3.7 billion visits per month, with an average of 6 minutes and 25 seconds per session.[1] It showcases the speed with which many people embraced AI chatbots for different tasks such as analysis of documents, assistance with job applications, and even emotional venting. Yet, with all these developing features in trust towards the AI system as an entity with personal information, the legal debate regarding users' rights–given consent or lack thereof–and security data, is taking its weight.

The use of artificial intelligence chatbots results in the uncontrolled processing and visibility of most private documents or sensitive information while posing serious threats on both legal and ethical fronts. The recent trend on TikTok has seen users employing AI platforms such as ChatGPT as personal therapists. In one example, a user enters personal journal entries into ChatGPT and then asks for an analysis and advice.[2] As seen from the example, despite the common knowledge to not "tell the internet anything personal about themselves", most users have little knowledge about how a chatbot actually stores or processes information–such as personal identification data, medical records, financial documents, and private messages–when

[1] Kseniia Burmagina, "ChatGPT Usage: Statistics and Facts," Elfsight, 2025, https://elfsight.com/blog/chatgpt-usage-statistics/.

[2] NewsGP, "Increase in Patients Turning to AI for Therapy," NewsGP, 2025, www1.racgp.org.au/newsgp/professional/increase-in-patients-turning-to-ai-for-therapy.

unknowingly inputting those.[3] From here, issues regarding the validity of the data consent process arise.

Moreover, the study has the aim of uncovering the extent at which private information - from casual confessions or personal confiding to the upload of confidential documents–is stored, reused, or exposed to the web by such AI chatbots. It asks a very fundamental question: when users share any kind of sensitive information to an AI chatbot, where does the information truly go and whether anyone is responsible for protecting it? This concern later on becomes particularly relevant, considering the history of Generation Z (or "GenZ") and their digital habits.

Even long before AI became a trend, GenZ has always been mostly known for expressing themselves openly online–whether it is through venting frustrations, narrating any personal experiences, or even forming emotionally vulnerable connections with strangers across social platforms. According to Maya Elizabeth Neufeuld-Wall from Digital Commons@Trinity, GenZ often utilizes social media platforms for self-expression and identity formation; including sharing personal experiences, emotions, and aspects of their daily lives online.[4] This forms communities and connections, encouraging an environment that allows vulnerable interactions in the search of support and understanding from their peers.

The vulnerability of Gen Z in this context stems less from their use of AI as a 'therapist' and more from the developmental intersection of identity formation and digital-first social architectures. Unlike previous generations, Gen Z's search for peer support often occurs in environments that incentivize radical transparency as a means of building community and validating personal experiences. When these

---

[3] Lorainne Martinengo et al., "Conversational Agents in Health Care: Expert Interviews to Inform the Definition, Classification, and Conceptual Framework," Journal of Medical Internet Research 25 (2023): e50767, https://doi.org/10.2196/50767.

[4] Neufeld-Wall Maya and Trinity University, "Being Real: Gen-Z, Self-Presentation, and Authenticity on Social Media," Digital Commons @ Trinity, 2023, digitalcommons.trinity.edu/cgi/viewcontent.cgi?article=1026&context=comm_honors.

users transition from public social platforms to the perceived private space of an AI chatbot, they carry over these habits of high-disclosure often seeking the immediate, non-judgmental validation that characterizes their online peer interactions. This creates a privacy paradox where the psychological need for emotional venting and introspective dialogue overrides the technical awareness of data permanence, making them a primary demographic for the unintentional collection of highly sensitive emotional data.

This situation is found even more urgent by the apparent rising trend on the use of AI chatbots for highly personal matters, such as emotional support or therapy sessions. For example, chat users often speak out about their experience with ChatGPT in evaluating personal journal entries or mental health experiences on platforms like TikTok–divulging intimate knowledge to systems whose data-handling policies are still at best, ambiguous.[5] For instance, a TikTok user was seen writing her thoughts into a word document before entering keywords containing instructions that reads as, 'read into the following journal entry and provide an analysis of it' into ChatGPT.[6] The user made use of ChatGPT as her personal friend or therapist, providing her with an analysis of her thoughts, feelings, constructive criticism, and more–'validating' her feelings and situations, acting as an online mental health counseling service. This occurrence indicates an increasing amount of trust among people who treat AI as a sort of friend or therapist, although the systems themselves have little, if any, confidentiality or ethical objectivity by which to judge professional standards in medical or psychological services. There is, of course, no regulation to put safeguards in place, meaning that users could be put under surveillance, find their data leaked, or have their findings accessed by third parties without their consent.

Furthermore, this trend is not only limited to casual conversation. Increasing numbers of users are uploading entire documents into these AI systems for assistance–whether it is to refine grammar, edit cover

[5] Caitlin Chin-Rothmann, "Protecting Data Privacy as a Baseline for Responsible AI," Protecting Data Privacy as a Baseline for Responsible AI, 2024, https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai.

[6] NewsGP, "Increase in Patients Turning to AI for Therapy."

letters, or enhance–or even aid in the creation of CVs ("Curriculum Vitae"). It displays TikTok users promoting a 'CV Builder' AI Chatbot where users only need to enter their data to create a professional and read-to-use CV. Such documents often contain full legal names, contact information, education and employment histories, and other personal details that are easily identifiable. The issue arises when users engage in such practices without a clear understanding of how AI processes or retains this information, with no assurance as well whether their data is kept confidential.

In reality (*das Sein*), users of all ages come to use AI Chatbots such as ChatGPT for a multitude of things–but mostly in the way a smart search engine is used. Due to ChatGPT's unique user interface with the appearance and simulated feel of messaging or chatting with a real person, a lot of users drop their guard and start to "be themselves" with the chatbot, allowing them to easily divulge sensitive and personal information such as personal details, emotional confessions, or even to ask for the chatbot to fix for any grammar mistakes of a highly sensitive document. Unbeknownst to them, without understanding how their data is processed, stored, or reused. AI developers, on the other hand, tend to value functionality and practicality over a strict safeguard of data protection which cracks up the differences between the manner in which consent and privacy policies are applied. This observation shows the imbalances between the expectations of privacy in users and behaviors of the AI system when sensitive information is often badly secured.

As such, the law of both Indonesia, Law No.27 of 2022 on Personal Data Protection (PDP Law), and the EU GDPR (Regulation (EU) 2016/679 on General Data Protection Regulation belong to providing the standard norms of data protection. The PDP Law provides that personal information can only be handled in accordance with valid permission to act, legal requirements or, justifiable interests, whilst the GDPR provides that permission should be explicit, informed, freely given and in any case, revocable, especially those classes of information that are sensitive in nature. Theoretically, these clauses are meant to ensure that the user is in control, the controller is accountable, and that there is a shield of protection against data abuse. The primary challenge lies in the regulatory lag between Indonesia's PDP Law and

the rapid deployment of Generative AI. While the PDP Law provides a foundational framework, its enforcement remains largely ineffective in AI-driven environments because the technology operates through decentralized data processing and complex algorithms that bypass traditional notice-and-consent models. These technical characteristics create regulatory loopholes where data controllers can exploit the lack of AI-specific definitions—such as those found in the EU AI Act—to process sensitive information under broad, non-specific legal bases. Consequently, without secondary regulations that specifically address automated decision-making and algorithmic transparency, the current legal protections remain theoretical rather than functional

Because the use of AI chatbots such as ChatGPT involves the input of sensitive personal data, the issue raised countless legal concerns surrounding its data privacy and user protection. The PDP Law, established in Indonesia, states a legal requirement for data controllers to only have the rights to process personal data once explicit consent is obtained from data subjects. Sensitive information categorized as health information, financial records, or private communications are types of data that AI chatbot users are often most unaware of inputting into the systems, where they are unknowingly processed, stored, or potentially even reused by the chatbots–without the user's explicit awareness or informed consent. Such an issue may result in possible violations of the PDP Law.[7] Moreover, because Indonesia has not yet established laws in regards to AI, there are no clear-cut laws regarding the use of AI and thus, rules and regulations for the processing of user data are still yet to come.

The law lacks specifics when it comes to automated data processing and how AI systems function, often creating a regulatory gray area that weakens the users' protection in practice. This can be further supported in Article 20 of the PDP Law where it states that, "Personal Data Controllers must have a basis upon which Personal Data is processed." The basis of Personal Data Protection speaks of valid consent from the

[7] Asean Breafing, "Indonesia's Comprehensive Personal Data Protection Law Guide - Indonesia Guide," Doing Business in Indonesia, 2025, https://www.aseanbriefing.com/doing-business-guide/indonesia/company-establishment/personal-data-protection-law.

Personal Data Subject, fulfilling legal obligations or obligations in accordance to agreement with Personal Data Subjects, or other justifications such as protecting vital interests or to serve legitimate interests with due regard to the purposes–none mention of any basis that AI has over data procession.[8]

From what can be seen by the PDP Law, it stipulates that data controllers are legally responsible for managing personal data in accordance with provisions under PDP Law.[9] On the other hand, the GDPR's stance on the collection of data is answered in Article 6(1)(a) of the GDPR in regards to Lawfulness of Process where processing data is only lawful if the data subject has given consent to the processing of his or her personal data for any specific purpose. As it can be seen, the GDPR's stance falls in line with the PDP Law in regards to user data consent processing.

However, unlike Indonesia, the European Union has already created a regulation on information privacy which is, the GDPR. At its core, the GDPR is designed to protect the personal data or any information of any identified or identifiable individual, as stipulated in Article 4(1) of the GDPR. Because of AI's machine learning that thrives on data, any use of behavioural patterns, facial recognition data, voice recordings, or even texts can be used and falls within the scope of GDPR.[10] When it comes to Large Language Models ("LLMs"), the GDPR demands for strict adherence if any data used belongs to an EU citizen. The GDPR focuses on any justifiable grounds for data management where explicit consent for the usage of personal data by AI models red: is required - green: is required, and that it must be guaranteed that the AI developers are given consent willingly by the data

---

8 Republic of Indonesia, "Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection" (2022).

9 Sri Pujianti, "Govt: Law on Personal Data Protection Provides Legal Protection," Constitutional Court of the Republic of Indonesia, 2023, https://en.mkri.id/news/details/2023-02-13/Govt:_Law_on_Personal_Data_Protection_Provides_Legal_Protection.

10 Oluwatosin Victoria Ademokun, "AI And the GDPR: Understanding the Foundations of Compliance," TechGDPR, 2025, techgdpr.com/blog/ai-and-the-gdpr-understanding-the-foundations-of-compliance.

used. Doing so ensures the rights of the data subject and removes any chance of the data being compromised.[11]

Moreover, the new regulation implements the principle of accountability, which requires data controllers or processors to prove their adherence to rules related to obtaining consents and data security provisions. Through this framework, not only can transparency and fairness be guaranteed when managing sensitive information but also can establish a more international standard of regulating AI technologies. As such, the GDPR effectively operates as a benchmark to jurisdictions such as Indonesia, where the PDP Law continues to remain in its early stages of establishment, due to its role in providing guidance as regards to how effective consent warranties and accountability can eliminate the threat of unregulated exposures through AI systems.

Although the comparative information on the PDP Law of Indonesia and the GDPR of the European Union points to the advantages and disadvantages to the existing regulating institutions, these laws should be tested in the real application, which typically concerns real-world events. The meaningfulness of the evaluation of the effectiveness of the data protection measures and the consent procedures can be conducted based on the practice, instead of on the principle. Case studies are also an important perspective through which it is possible to test whether the requirements and expectations toward the data controllers, processors and AI developers achieve any success in the protection of private and sensitive data. Specifically, analyzing the latest security breaches associated with AI chatbots, including theft of ChatGPT user credentials, one may see the discrepancies between *das Sollen* and *das Sein*.

A cybersecurity company, Group-IB from Singapore was discovered to have 101,100 devices infected with malware, making it possible to save ChatGPT login data. The following data was then found to be collected and sold and traded on dark web marketplaces.[12]

---

[11] Exabeam, "The Intersection of GDPR and AI and 6 Compliance Best Practices," Exabeam, 2025, www.exabeam.com/explainers/gdpr-compliance/the-intersection-of-gdpr-and-ai-and-6-compliance-best-practices/.

[12] GROUP-IB, "Group-IB Discovers 100K+ Compromised ChatGPT Accounts on Dark Web Marketplaces; Asia-Pacific Region Tops the List," GROUP-IB, 2023, www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials.

The number of available logs that contained ChatGPT accounts reached a peak of 26,802 in May 2023. According to findings by Group-IB, this was the highest concentration of ChatGPT account data offered for sale over the past year. These info-stealing malware managed to harvest the credentials or data stored, allowing the stealers to pick up saved login information, browser cookies, bank card details, browsing history, and even other information from browsers. Because ChatGPT, by default, retains users' chat history, means that there will always be a risk of exposing private or sensitive content stored by the users. In addition to that, employees within organizations have started using ChatGPT whether it is for software development or business communication, potentially exposing confidential or sensitive information which can be exploited to attack companies and its employees.[13] The fact that 101,000 ChatGPT Accounts were stolen and sold on the dark web markets shows a clear poor handling of safeguarding user's chat history and data, which includes sensitive personal information. The theft in the case demonstrates how consent alone is not enough if there are failures in the security framework. As such, it shows how the use of AI Chatbots could potentially expose sensitive data in ways that regulation doesn't cover.

The main aim of the research is to critically evaluate the legal status of AI chatbots in Indonesia in the framework of the PDP Law and the GDPR that regulates the European Union. This includes examining whether chatbots can be considered as legal subjects in their own right, or whether they can be thought of as tools in the control of data controllers and processors. It is essential to fully understand this stance, as the establishment of legal standing determines the matter of accountability and liability when it comes to the question of personal data misuse or uncontrollable disclosure.

Another goal is the assessment of the consent to the data validity process when AI chatbots retrieve personal and sensitive data, including casual user data disclosure, as well as uploading confidential documents. Through an exploration of the consent frameworks required by both the PDP Law and GDPR, the paper aims to assess whether the frameworks can offer any real protection to data subjects in an artificial intelligence-

[13] GROUP-IB,

driven world. Overall, the general objective is to investigate the soundness of these consent procedures and define whether they will successfully help to protect individuals against the threats of uncontrolled disclosure.

With that being said, it is imperative to formulate a robust legal and policy framework that ensures AI chatbot technologies functioning well within proper boundaries concerning data privacy and protection. The reforms should require organizations to clearly state how they handle and use online data, motivate developers to complete data protection impact assessments and grant users some control over their data.[14] Assessing how limited Indonesia's rules in comparison to the GDPR can highlight what measures should be taken to promote the safety of users of such applications. Moreover, the GDPR includes principles of accountability that undermine the process of proving the legality of the consent requirements and the data protection measures on data controllers and processors.

The paper discusses the legal risks of AI chatbots in terms of the protection of personal data, especially in terms of uncontrolled disclosure of private documents and sensitive data according to the PDP Law. The impact of artificial intelligence in processing data for personal use is assessed with the legal implications of the user's willingness to share personal information online, along with the regulatory gaps that expose the data to vulnerabilities. Furthermore, this study underlines that the AI cannot be evaluated exclusively within the paradigm of the PDP Law but also to be evaluated in the context of international regulations, including the GDPR, wherein comparative analysis is of essence in order to develop a proper set of hypotheses.

Taking all the issues together, the recent integration of AI chatbots including ChatGPT has produced a completely different virtual space with the situation when personal and sensitive information is actively exchanged by users, and it is usually done without sufficient awareness of the outcomes. The dangers of uncontrollable disclosure no longer exist in theory as demonstrated by user behavior, generational digital

[14] Yudhi PrasetyoReza Aminy, "Introduction of the Official Personal Data Protection Act (UU PDP)," BDO, 2024, https://www.bdo.co.id/en-gb/insights/introduction-of-the-official-personal-data-protection-act-(uu-pdp).

behavior, and even large-scale credential theft cases. Although both the PDP Law of Indonesia and the GDPR of the European Union have setups, which focus on consent, accountability and user rights, the discrepancy between normative code and the actual reality of using AI evolves conflicts, anomalies and loopholes that the existing legislation is not well-prepared to tackle.[15] This friction highlights the fact that it is essential to re-evaluate the operation principle of legal protections under the situation when AI creators, data handlers, and users assume important roles. Thus, this study will find its place to be the law-technology-society responsibility as it seeks various answers to how legal frameworks are sufficient even to the present stating that a future way forward needs to offer more solutions to the problem of personal data protection that can be equitable and enforceable in the era of artificial intelligence.

Drawing from the preceding background, this research formulates the following key inquiries: (1) How do the PDP Law and the EU GDPR compare in their regulatory approaches to Private and Sensitive Information?; and (2) How is the validity of consent determined when Private and Sensitive Information is collected by AI Chatbots?

The objectives of this research are grounded in two primary aims: addressing contemporary legal challenges and enriching legal theory, by, first, assessing the regulatory frameworks of the PDP Law and EU GDPR, identifying and mitigating legal uncertainties caused by gaps in current legislation, and second, evaluating the validity of consent in the context of AI Chatbots, thereby offering theoretical contributions to the evolution of data protection law.

This research adopts a normative legal research framework, which views law as a system of norms and examines rules, principles, and doctrines to resolve legal issues. This approach seeks to identify, analyze, and systematize legal norms through a doctrinal method. Three methodological approaches are applied: statutory and comparative law, examining relevant legislations which are: i) Law of

[15] Martin Hasal, Jana Nowaková, Khalifa Ahmed Saghair, Hussam Abdulla, Václav Snášel, and Lidia Ogiela, "Chatbots: Security, Privacy, Data Protection, and Social Aspects," Concurrency and Computation: Practice and Experience 33, no. 19 (2021): e6426, https://doi.org/10.1002/cpe.6426.

the Republic of Indonesia Number 27 of 2022 on Personal Data Protection; ii) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data; iii) Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence; and iv) OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Annex to the Recommendation of the Council of 23 September 1980, as revised on 11 July 2013).

The legal materials for this research were collected through a comprehensive desk-based library search, involving a systematic review of primary and secondary legal sources. Primary sources consist of Law No. 27 of 2022 (Indonesian PDP Law) and the EU General Data Protection Regulation (GDPR). Secondary sources include academic journals, law books, and relevant international reports. The collection process utilized a purposive sampling technique, prioritizing the most recent regulatory updates and scholarly discussions concerning artificial intelligence and automated data processing.

The analysis of legal materials is conducted using a qualitative-normative technique, specifically through a comparative synthesis. The study juxtaposes the legal bases for data processing—specifically Article 20 of the Indonesian PDP Law and Articles 6 and 7 of the GDPR. The synthesis is performed by deconstructing the elements of valid consent and legitimate interest within both frameworks to determine their applicability to automated environments. By identifying the normative friction between these provisions, the research evaluates whether the Indonesian framework offers a 'functional equivalence' to the GDPR standards or if there are structural gaps that necessitate regulatory reform in the context of AI chatbot operations.

B. The Legal Frameworks Compared: PDP Law *vis-à-vis* EU GDPR on Sensitive Information

The concept of Personal data protection is based on a wider legal and philosophical background of the right to privacy. In the age of digitization when a continuous process of gathering, processing and

distributing of personal data occurs within the framework of technology use, the issue of safeguarding this information has become a legal necessity. Personal data as defined by the European Commission states that, "Personal data is any information that relates to an identified or identifiable living individual (data subject). Different pieces of information, which together can lead to the identification of a particular person, may also be considered personal data."[16]

Domestic law and international norms, namely the General Data Protection Regulation ("GDPR") and the Privacy Principles of the Organisation for Economic Co-operation and Development ("OECD") have been the most significant influence in the evolution of data protection theory, which establishes a normative approach to the processing of personal data with transparency, fairness, and respect to individual autonomy.

The key component of the personal data protection theory are the legal requirements that bind data handlers, who are usually called data controllers and data processors. ICO states that the controller of the data is the party that decides about the purposes and methods of processing of personal data, and the processor processes the data upon the request of the controller. The actors are also liable to certain legal obligations, including the obligation to maintain accuracy of data, using data only as stated, with clear purposes, and to exercise reasonable security practices. For instance, in the GDPR, there are seven pillars of data processing including: Fairness and transparency; Purpose limitation; Data minimization; Accuracy; Storage limitation; Integrity and confidentiality; and Accountability.[17] The same principles are reflected in the data protection framework of other countries, such as Indonesia, where under the PDP Law, data controllers are put under obligation to ensure the secrecy, soundness, and accessibility of personal data.

[16] European Commission, "Data Protection Explained," European Commission, 2025, https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.

[17] ICO, "A Guide to the Data Protection Principles," ICO, 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/.

The principle of consent is one of the frameworks of data protection. According to international laws, such as the GDPR, a valid consent should be freely provided, specific, informed, unambiguous, and requires a positive affirmative act of the data subject.[18] The principle seeks to protect the individuals autonomy by guaranteeing individuals control of their personal data. The OECD Privacy Principles also give weight to knowledge and consent especially when it comes to data collection and disclosure.[19] Any data processing procedure can be potentially regarded as a threat to individual privacy rights and the lack of meaningful consent jeopardizes the trust of people in digital systems. The importance of consent could also be seen in the national laws like the PDP Law in Indonesia, where it is stated in Article 20(1) that personal data must not be used or distributed without the authorization of the data subject.[20] Nevertheless, the existence of AI cannot replace data controllers due to the nature of data subjects where consent must only be taken directly from the data subject, and interested parties.

The basic privacy rights, as quoted directly from Cornell Law School LII, are core to the theory of personal data protection. These rights include the right to information, access rights, rectification right, erasure right and the right to object to processing of data.[21] These rights are known to be an extension of the right to privacy and they guarantee individuals, or users, a meaningful control over the use, sharing, and storage of their data. These rights are formalized in the United Kingdom under Article 5(a) of the UK GDPR, where it is outlined in its guidance for organizations that process personal data–that the data must be processed lawfully, and transparently. On the same note, the data protection and privacy principles adopted by the United Nations legitimize that the data subjects should be able to access effective

[18] General Data Protection Regulation (GDPR), "Consent - General Data Protection Regulation (GDPR)," 2024, https://gdpr-info.eu/issues/consent/.

[19] Rob Witcher, "OECD Privacy Guidelines & Security | CISSP Study Guide," Destination Certification, 2025, https://destcert.com/resources/oecd-privacy-principles-global-security/.

[20] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, Article 20 (1).

[21] LII (Legal Information Institute), "Right to Privacy," LII, 2025.

remedies and protections, especially where their data rights are violated or misused.[22]

The GDPR and the OECD Privacy Guidelines are examples of international frameworks that contributed immensely to the shaping of international data protection standards. The GDPR, which can be called the 'gold standard of data privacy regulation', introduces the rights-based approach, putting the individual at the center of all activities involving data. More modern data governance was founded on the OECD Privacy Principles, which were initially set forth in 1980 and subsequently revised, which introduced many of the primary norms still in use today, including data quality, purpose specification, security safeguards, and accountability.[23] All these frameworks are used to gain a theoretical and legal basis by countries that are in the process of formulating or strengthening their local data protection laws, such as Indonesia, whose PDP Law echoes most of the same principles and duties.

The scope and definition of private and sensitive information can change under different privacy laws–hence the PDP and EU GDPR laws would naturally contain different definitions of personal information. In this study, these definitions will be thoroughly explored and compared against, in order to take note of legal gaps within regulation. Personal information overall can be defined to be data that can directly or indirectly identify an individual or household. Sensitive data on the other hand, is able to determine information such as a person's opinions, personal preferences, or any other susceptible details that may lead to identity theft, fraud, or harm if the data happens to be leaked, breached, or compromised.[24] As stipulated in Article 4 (1)(2) of the PDP Law, Indonesia divides personal data into two categories,

---

[22] United Nations - CEB, "Principles on Personal Data Protection and Privacy," United Nations - CEB, 2025, https://unsceb.org/principles-personal-data-protection-and-privacy-listing.

[23] Ece Gumusel, "A Literature Review of User Privacy Concerns in Conversational Chatbots: A Social Informatics Approach," Journal of the Association for Information Science and Technology 76, no. 1 (2024): 121–54, https://doi.org/10.1002/asi.24898.

[24] TermsFeed, "Personal Vs. Sensitive Personal Information," Termly, 2025, https://termly.io/resources/articles/sensitive-personal-information/.

namely, general and specific types of personal data. The general category of personal data includes knowing the full name, gender, citizenship, religion, and other types of data that allows the identification of a person.[25] On the other hand, specific personal data includes medical information, biometric data, genetic data, personal financial data, criminal records, and data on children as well as 'other data under law and regulation'.

In comparison, the EU GDPR does not divide personal data into two categories unlike the PDP Law, however it has a more comprehensive and descriptive definition on personal data. It can be seen on Article 4(1) that 'personal data' refers to information that relates to an identified or identifiable natural person ('data subject'). The identifiers are ruled as follows: identification number, location data, online identifier whether physical, physiological, genetic, mental, economic, cultural or social identity.[26] Additionally, the EU GDPR classifies certain types of data into special categories that includes racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, and biometric data–according to Article 9(1).[27]The following categories that have been mentioned require prior permission in order to process, which thus establishes the thorough protection of the following sensitive data.

When comparing both laws on the comparative treatment of sensitive data, the initial scope and definitions are quite similar. In terms of data protection, both the PDP Law as well as the EU GDPR employ terms such as "Special Categories of Personal Data" (GDPR) and "Specific Personal Data" (PDP Law) in order to designate as "Sensitive Data". As previously mentioned, if the data can be linked to an identifiable person, then it is considered as sensitive data and therefore requires a high level of protection according to regulation. How sensitive data should be treated in both PDP Law and GDPR, should share the fundamental principle of enhanced safeguards. However, it

[25] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, Article 4(1)(2).

[26] Regulation (EU), "Regulation (EU) 2016/679 (General Data Protection Regulation)" (2016).

[27] Regulation (EU) 2016/679, Article 9(1).

differs when it comes to its legal starting point for processing data as well as compliance measures.

In contrast, the PDP Law requires processing activities to be grounded in a lawful basis which includes: explicit consent, contractual necessity, fulfillment of law requirements, safeguarding of vital interests or public service. The processing of Personal Data is still allowed as long as there is a basis for it, but with an additional duty for controllers and processors to make it confidential and secure.[28] Both frameworks especially stress on the role of explicit consent as a pillar of lawful processing of sensitive data. Under the EU GDPR, the consent to processing 'Special Categories', as previously mentioned, is required to be a higher standard than for normal personal data–it must be freely given, specific, informed and using a clear affirmative action, allowing no room for doubt as to the reason of the processing of personal data (Article 4(11)). Likewise, the requirement of explicit and written or recorded consent laid down by the PDP Law closely follows the requirements of the GDPR in terms of informed and specific consent (Article 20(1)(2)).[29] Both of the regulations require controllers to assess the risk and implement measures in order to manage the risk related to high-impact data processing. The GDPR requires that a Data Protection Impact Assessment (DPIA) should be conducted where the processing of personal data would most likely play a larger risk to individuals–including, by where large-scale processing of Special Categories of Data is concerned, as stipulated in Article 35(3) of the GDPR. Meanwhile, Article 34 of the PDP Law follows a similar route, where personal data controllers must make impact assessments on the processing of Personal Data which may be categorized as "high potential risk" to the rights of the data subject. In Article 35(2), it specifically mentions that the personal data processed with high risk may include the processing of 'Special Category' personal data as well as large-scale personal data. The processing of Specific Personal Data is considered to be a "high potential risk" activity, where the data subject has the right

[28] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, Article 20.

[29] Regulation (EU), Regulation (EU) 2016/679 (General Data Protection Regulation), Article 4(11) and Article 20(2).

to be informed and mentioned, whereby controllers are required to carry out and evaluate impact assessments on such a basis.

Another area where both regimes are the same but differ in degree, is the requirement to appoint a Data Protection Officer (DPO). Under Article 37(1)(c) of the GDPR, a Data Protection Officer (DPO) is required when an organisation performs on a large scale of Special Categories of Data or data related to Article 9 or 10.[30] In the PDP Law, the DPIA's intervention is considered to be 'conditional', as stipulated in Article 39 on the specific circumstances: the need to have a DPO arise in the case of organizations performing main activities concerning large-scale processing of Personal Data, for data public services or for systematic monitoring of people. The scope of any additional safeguards are also discriminating in prescriptiveness. The GDPR offers a very detailed framework, requiring controllers to implement technical and organisational measures–including strict access controls, data minimisation, encryption and comprehensive record keeping of processing activities or processed data–in order to respect the rights and freedoms of data subjects (Art. 24-32).[31] The PDP Law, on the other hand, stipulates a greater need for security and compliance procedures when dealing with Specific Personal Data, though the law is not yet detailed enough to insert a similar process rule. It does however tie the processing of such data to mandatory DPIA and DPO obligations as it secures Indonesia's shift to a risk-based compliance framework as opposed to rule-based prescription.

Despite the conceptual equivalence, the distinction between sensitive and specific data classification is not completely the same between the two regimes. Under the GDPR, race, ethnicity, political beliefs, and sexual orientation are automatically considered sensitive and hence impose severe processing limitations. On the contrary, the PDP Law does not necessarily regard such identity-based features as necessarily sensitive, e.g., religion or nationality might be counted as general personal data under the Indonesian regime. This proves that the level of sensitiveness to be given on certain forms of data is relative and it is determined by the sociocultural and legal context of individual

[30] Regulation (EU) 2016/679, Article 37(1)(c).
[31] Regulation (EU) 2016/679, Article 24-32.

jurisdictions. This results in the fact that not every type of data seen as special in the GDPR is necessarily seen as a special one in the Indonesian legislation. Unlike the GDPR, the Indonesian PDP Law includes financial data under the specific data category but remains silent on the specific protection of religion and nationality, which may expose users to heightened risks of discriminatory AI profiling as explained on Table 1.

TABLE 1 Type of Data Comparison between the EU GDPR and PDP Law

Type of Data	GDPR (Special Category of Personal Data)	PDP Law (Specific Personal Data)
Racial/Ethnic Origin	✓	x
Political Opinion	✓	x
Religious Beliefs	✓	x (General Data)
Trade Union Membership	✓	x
Biometric Data	✓	✓
Health Data	✓ (and sexual orientation)	✓
Genetic Data	✓	✓
Data on Children	x (Art.6(1)(f) and Art.8)	✓
Criminal Records	x (Art.10)	✓
Personal Financial Data	x	✓

Source: synthesized by the authors directly from the primary statutory texts of the EU GDPR and Indonesia's UU PDP (Law No. 27/2022). For the European framework, the classifications were mapped using Article 9(1) for special categories of personal data, alongside Articles 8 and 6(1)(f) for children's data, and Article 10 for criminal convictions. For the Indonesian framework, the data was extracted from Article 4 Paragraphs (1) and (2) of the UU PDP, which delineates general data from specific personal data, relying on the explicit statutory enumeration of sensitive categories set forth in Article 4 Paragraph (2) letters a through g.

The discrepancy in data classification between the GDPR and the Indonesian PDP Law reflects a fundamental difference in regulatory philosophy. While the GDPR prioritizes an intrinsic dignity-based approach—classifying data as 'special' if its misuse inherently violates

fundamental human rights—the Indonesian PDP Law adopts a more functional-pragmatic approach. By categorizing financial data as 'specific' (sensitive) data, Indonesia acknowledges the immediate socio-economic vulnerabilities of its citizens to digital fraud. However, this pragmatism creates a legal imbalance: by excluding categories such as religion or nationality from the 'specific' designation, the PDP Law inadvertently lowers the threshold for legal protection against non-financial harms, such as algorithmic bias.

Moreover, The legal implications of this classification are profound when examined through the lens of AI-driven profiling. If religion or nationality are treated as 'general' data under the Indonesian framework, AI controllers may process these data points without the rigorous Data Protection Impact Assessment (DPIA) or the explicit consent requirements mandated for specific data. This oversight creates a fertile ground for discriminatory profiling, where AI chatbots or processing systems may generate biased outputs that marginalize certain religious or ethnic groups. Under the current PDP Law, victims of such discrimination would face a higher evidentiary burden, as they cannot invoke the stricter liability standards associated with the misuse of specific data. Consequently, there is an urgent need to reclassify these 'social identifiers' as specific data to prevent AI systems from automating systemic discrimination under the guise of general data processing.

One of the major differences between the two regulations is the extent to which each law deems something to be sensitive. As shown in Table 1, Racial or ethnic origin, political opinions, religious beliefs, and sexual orientation have been listed as Special Categories of Data in the GDPR, as they are directly related to the discrimination and freedom of the person (Art.9 GDPR).[32] By contrast, the Indonesian PDP Law is more pragmatic, not including all of these categories in its definition of Specific Personal Data. Rather, it also contains personal financial data, information about children, and criminal records–which are not explicitly mentioned in the GDPR but identified in other regulations such as Articles 8 and 10.[33]

[32] Regulation (EU) 2016/679, Article 9.

[33] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, Article 4.

It is important to note that religion and nationality are treated as 'General Personal Data' instead of 'Sensitive Categories' under the PDP Law, which is a large observation as compared to the GDPR's focus on basic rights and non-discrimination. Such a difference corresponds to a variety of cultural and regulatory contexts, as the EU values the protection of the identity-based features that might result in discrimination whereas Indonesia values information that has possible financial or social vulnerability consequences.[34] Both regulations demand increased security and clear consent as well as stronger accountability in processing such information; processing under the GDPR is prohibitive in nature (it must be justified by one of the exceptions listed in Article 9(2)). Under the PDP Law on the other hand, processing personal data must be collected in a lawful, fair and transparent manner with purpose and guaranteed rights of the personal data subject, and other rules of consent, as stipulated in Article 16 of the PDP Law.[35] The main difference is that the sensitive information in each of the legal systems is treated differently. The processing of special categories of personal data is by default forbidden under the GDPR unless it falls within one of the few exceptions of Article 9(2) based on a rights-based strategy which is grounded on the principles of non-discrimination and human dignity. The PDP Law, meanwhile, is risk-based and conditional. Due to increased risks, more rigorous procedural safeguards should be observed in the processing of sensitive or specific personal data, and automated processing without human oversight should be avoided in most cases, to avoid discriminatory or other detrimental outcomes.

Additionally, the EU holds a strong emphasis on fundamental freedom as a philosophical and legal driving force for the GDPR. According to Recital 1 of the EU GDPR, it defines that the protection of natural persons with respect to the processing of personal data is a fundamental right, based on Article 8 of the Charter of Fundamental

[34] Valentina Ancillia Simbolon and Vishnu Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation," *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (2022): 178–90, https://doi.org/10.31314/pjia.11.2.178-190.2022.

[35] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, Article 16.

rights, which ensures both privacy and data protection as indivisible freedoms.[36] This presents data protection as the continuation of human dignity and autonomy as opposed to a regulatory issue. Moreover, it is also stated in Recital 2 that Recital 1 links directly to establishing an "area of freedom, security and justice", which ensures the free movement of personal data across Member States to not be hindered by any inconsistent national laws–whereas Recital 4 specifies that other fundamental freedoms, freedom of expression and carrying out the business, should also be guiding the exercise of this right.[37]This means that under the GDPR, the principle of data protection is also a fundamental right, where the personal data will not be separated from a person's dignity and autonomy (it uses a rights-based model where safeguards have already been established to ensure the maximum level of data protection). As such, the processing of personal data is strictly limited, especially in 'Special Categories' where it is already prohibited by default, unless justified by any exceptions under Article 9(2). Additionally, this also reflects the EU's Recital 2 of maintaining "an area of freedom, security, and justice" where the rights of individuals will not be compromised although the data moves freely across borders. On the other hand, the PDP Law does not frame data protection to be a fundamental right, but more of a mechanism for the sake of ensuring fairness, transparency, and accountability in governance, hence making use of a more risk-based approach which focuses more on the mitigation of any potential harm such as financial loss or reputational damage. As so, the EU GDPR is more rights-oriented whilst the PDP Law focuses more on a consequence-oriented approach.[38]

Although the EU GDPR does not differentiate personal data into categories like the PDP Law, it still describes the type of special data that requires special requirements in order to be processed. In addition to that, although the PDP Law and EU GDPR has a common aim of

[36] Regulation (EU), Regulation (EU) 2016/679 (General Data Protection Regulation), Recital 1.

[37] Regulation (EU) 2016/679, Recital 2 and Recital 4.

[38] Muchamad Taufiq and Ananda Salsabila Kenyo, "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR," *International Journal of Business, Law, and Education* 6, no. 2 (2025): 1260–68, http://ijble.com/index.php/journal/article/view/1178.

guaranteeing the safety of data subjects from any misuse of data, there are still gaps in terms of the data processing aspects. The GDPR clearly states that it is not allowed to process sensitive data unless there are special requirements (Art.9), as previously mentioned, but the PDP Law does not elaborate on the parameters of processing sensitive data. This contrast shows that there is a gap in the law that may potentially expose Indonesian users' personal data–during the use of AI chatbots, giving vulnerability of becoming a profiled identity which may potentially make users subject to theft or involved in unwarranted disclosures. In turn, the comparative study of these definitions does not only indicate the breadth of the legislation of both legal instruments but will also help to realise, wherein the Indonesian law has to be improved to comply with more detailed and strict protection provisions in the European Union's GDPR.

Thus, the scope and definition of what is private and sensitive information provides a basis for data protection regimes. Both the PDP Law and the EU GDPR define what constitutes as personal or sensitive data; by offering a clear definition and a set of guidelines for the way in which such data should be handled in practice. Yet definitions are not enough; its real value lies when they grant data subjects the proper rights to their personal data–enabling individuals to have control over accessing, processing and the retention of their information.

C. Rights and Obligations of Data Subjects on General and Sensitive Data

The rights and obligations of a personal data subject are central when it comes to data protection, as it contains the right that individuals are not just possessors of information, but also active participants in the decision-making process as to how their data can be accessed, processed, and shared. Both the PDP Law and the EU GDPR codifies such rights. However, the scope, granularity, and enforceability of such rights may differ between the two regulations.

As stipulated by Article 1(6) of the PDP Law, 'Data subjects' refer to individuals that the personal data relates to. These include the rights to be entitled to the information on their full identity, the legal grounds of request, use of Personal Data, and accountability of the party

requesting such data (Art.5).[39] In addition to that, personal data subjects shall have the rights to complete or update inaccuracies (Art.6), access or obtain a copy of their personal data (Art.7), the right to end, erase, or destroy personal data within law and regulation (Art.8), and the right to withdraw consent (Art.9).

Additionally, they also have the right to object to certain processing or profiling and the right to file for an objection and automated processing under regulation (Art.10) as well as the right to claim or recover damages in the case of a breach and claim for compensation as well (Art.12), the right to acquire or use personal data under certain conditions, transmit data to another Personal Data Controller (Art.13).[40] Whilst the law entitles such rights, however so, the absence of actual procedural details on how these rights can be enforced including all the details or requirements that must be met in order for such laws to meet eligibility in practice, are not explained in detail; especially in the context of Artificial Intelligence (AI) as well as automated processing–leaving uncertainty in terms of practical use. Even then, the previously mentioned Articles (8, 9, 10(1), 11, 13(1)(2)) are considered exempt under Article 15 in the case of interest of national defense and security, law enforcement, public interest, supervision of financial or administrative sectors of state, as well as for the purpose of statistical and scientific research–where the exemptions are only applied to enforce the laws.[41] Thus far, there has been no mention of AI in the first sections of the regulation.

Additionally, the PDP Law does not introduce a comprehensive ban on processing 'Specific Personal Data', rather it focuses on the obligations and requirements of the controllers. Article 4 outlines the Specific Category Personal Data which includes health, biometric, genetic, criminal records, children, and financial data. Indonesia has a more practical approach like for example, it is not a prohibition based on rights, but risk management and accountability.[42] Article 34 is a

[39] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, Article 5.

[40] Law 27 of 2022.

[41] Law 27 of 2022, article 15.

[42] Simbolon and Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation."

DPIA with high-potential risk processing, such as in relation to particular personal data, processing being of large scale, monitoring, or automated decisions. Article 35-39 and Article 54 are used to regulate the security, confidentiality and the role of the DPO/protection officer. Article 40 requires controllers to stop the processing in case the consent is revoked (except in a few cases), whereas Article 46 obligates them to notify data subjects and supervisory authorities within 3x24 hours of a breach.[43] As Taufiq et al. points out, the PDP Law focuses on transparency, fairness, and accountability on a risk-based framework, instead of making data protection a fundamental right.[44]

The EU GDPR, on the other hand, provides a more substantive and enforceable framework for the rights of data subjects. Chapter 3 on the Rights of the Data Subject consists of 5 different sections featuring: transparency and modalities, information and access, rectification and erasure, right to object and automated individual decision-making, and restrictions. From the get-go, it is already clear that the EU GDPR's regulations are far more detailed in comparison to the PDP Laws. Moreover, to further analyze the GDPR, Article 12 starts off with the transparency in information and proper communication between the Personal Data Subject with the Personal Data Controller where the Personal Data Subject has the right to information on how their data is processed in a concise and transparent manner–which will be further discussed in Sub-chapter 4.2.3 where the Obligation of Data Controllers and Processors come into play. Furthermore, Articles 15 to 23 forms a substantial set of rights: the rights of access (Art.15), rectification (Art.16), erasure or "right to be forgotten" (Art.17), restriction of processing (Art.18), notification of any erasure of personal data (Art.19), data portability (Art.20), the right to object (Art.21), and automated individual decision-making, which includes profiling (Art.22).[45] Importantly, Article 22 gives individuals protection against automated decision-making, such as profiling which directly concerns

[43] Articles 34-39, 40, 46 and 54 Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection.

[44] Taufiq and Kenyo, "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR."

[45] Regulation (EU), Regulation (EU) 2016/679 (General Data Protection Regulation), Articles 15, 16, 17, 18, 19, 20, 21, 22.

AI systems, such as chatbots. These rights are not abstract: they come with GDPR's clear obligations for controllers to comply with requests in a specified period of time, for their compliance to be subject to redress and support by supervisory authorities, and for GDPR's impositions of penalties for non-compliance.[46] In this respect, the GDPR empowers the rights of data subjects to the proper effective rights of autonomy and protection.

As referred to in Table 1 on the Type of Data Comparison between the EU GDPR and PDP Law, the GDPR places a special prohibition when processing 'Special Categories' of data (such as race, political opinions, religion, health, biometric, and genetic), unless there are exceptions applied in accordance with Article 9(2) GDPR (which includes explicit consent, public interest, and vital interests). Additionally, Article 6 presents the general lawful grounds of processing (consent, contract, legal obligation, public interest, legitimate interests), and also any processing of sensitive data should meet the requirements of Article 6 as well as Article 9. To ensure automated decision-making, Article 22 offers a specific right to the data subject not to have the decision made based on automated processing alone with legal or other similarly urgent outcomes. Additional procedural protection can be found in Article 35 where it provides a Data Protection Impact Assessment (DPIA) of high-risk processing (particularly of sensitive data) and in particular, focuses on the processing with the use of new technologies, and Article 37 proposes the appointment of a Data Protection Officer (DPO), in case the core activities of the controller are large-scale processing of special categories.[47]

Diving deeper into the EU GDPR Articles individually in comparison to the PDP Law, it can be observed in Article 15 of the GDPR that the data subjects are granted the right to obtain confirmation from the controller of whether personal data is being processed, access to such data, and additional data that includes the purpose of processing, categories of personal data, recipients of disclosed data, retention periods, rights to request of erasure or restriction of process, and safeguards on automated decision-making, which includes

[46] Regulation (EU) 2016/679, Articles 12, 13, 14.
[47] Regulation (EU) 2016/679, Articles 35, 37.

profiling.[48] Additionally, it also provides the right to copy data, where the first copy is free of charge, and the next at an additional but reasonable cost by the data controller, as well as the data being provided through electronic means (Art.15(3)). A similar Article is found in Article 7 of the PDP Law where the Data Subject also has the rights to access and obtain a copy of Personal Data. Nevertheless, contrary to GDPR, the PDP Law is not as detailed in the breadth, such as the cost of extra copies or the form of delivery, which is a problem that the GDPR solved.

The EU GDPR and the PDP Law of Indonesia acknowledges the focus on data subject rights in the protection and accountability of processing personal data, however, they have significant differences in its orientation, scope, and enforceability. The GDPR is a rights-based approach that has the protection of human dignity, autonomy, and non-discrimination in its foundation–providing a full set of rights that have to be enforced (especially in relation to automated decision-making and special category data), as previously mentioned. In comparison, the PDP Law is more risk-based and procedural in nature which emphasizes more on fairness, transparency, and accountability in handling and managing data rather than on innate personal rights. Although the Indonesian regulation mentions the most important data subject rights, including access, correction, erasure, and withdrawal of consent, the absence of procedural detail and enforcement strategies makes it a weaker aspect of the digital and AI-focused environment.[49]

Therefore, reducing the differences between the two laws, the effectiveness of the safeguarding of personal data would have to depend on how effective its implementation will be as well as its strictness in the controller's requirements. From here, this brings another important point of comparison–in terms of rights, obligations, function, and role of data controllers and processors. It is important to understand how each of the legal regimes manages these roles since they play a major part

[48] Regulation (EU) 2016/679.

[49] Eugene Bagdasarian, Ren Yi, Sahra Ghalebikesabi, Peter Kairouz, Marco Gruteser, Sewoong Oh, Borja Balle, and Daniel Ramage, "AirGapAgent: Protecting Privacy-Conscious Conversational Agents," in Proceedings of the ACM Conference on Computer and Communications Security (CCS '24), December 9–13, 2024, DOI:10.1145/3658644.3690350 (also available as arXiv:2405.05175)

in how the subject data is handled and processed, and to ensure that general and sensitive (specific or special categories) of data are handled lawfully and transparently.

D. Rights, Obligations, Function, and Roles of Data Controllers and Processors

As previously stated, both the GDPR as well as the PDP Law regimes take charge in the regulation of two main types of data which are general and special categories of data (GDPR) as well as personal data and specific data–both special categories (GDPR) and specific data (PDP Law) which are equivalent to sensitive data. The privacy of sensitive data are both directly connected to the rights of the data subject, but especially so, considered to be the duty and responsibility of the individuals controlling and processing such information–the data controllers and data processors. The PDP Law as well as the GDPR adheres to this by having separate but complementing sections of regulations, addressing the rights, obligations, roles, and function of both data controllers and data processing. Although the personal data can be defined as alike in nature in both regimes, the degree of protection and accountability in data controllers and data processors, depends on clauses. These clauses are intended to guarantee that data processing is performed in a way that is both lawful, fair and transparent, adhering to the principles of accountability and data minimization.[50] The reason for this is due to the GDPR's employance of a more rights-based model that comes with special regulations on special categories of personal data, whilst the PDP Law is a more risk-based model, which employs safeguards when specific personal data is involved.[51] Nonetheless, even with their similarity, the scope, enforceability, and practicality of these responsibilities vary considerably across the two systems.

---

[50] Laurie Carmichael, Sara-Maude Poirier, Constantinos K. Coursaris, Pierre-Majorique Léger, and Sylvain Sénécal, "Users' Information Disclosure Behaviors during Interactions with Chatbots: The Effect of Information Disclosure Nudges," Applied Sciences 12, no. 24 (2022): article 12660, https://doi.org/10.3390/app122412660.

[51] Taufiq and Kenyo, "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR."

According to PDP Law on General Provisions of Article 1(4) and (5), a Data Controller (*Pengendali Data Pribadi*) refers to an individual, a public body and an international organization that acts individually or collectively in order to define its purpose and control the processing of Personal Data. In the meantime, a Data Processor (*Prosesor Data Pribadi*) is a person who processes data on behalf of the Data Controller.[52] It is first mentioned in Article 18 of how up to 2 (two) Personal Data Controllers may process personal data by following the minimum requirements: an agreement among personal data controllers, defining role, responsibility, and relationship, purpose and method of processing, and a contact person. This then opens up to Chapter VI of the Obligations on Personal Data Controllers and Processors in the processing of Personal Data. The chapter opens up with Article 19 on how controllers and processors include any person, public bodies, or international organizations. Then moving on to Article 20 on the obligations of Personal Data Controllers, it is stressed that Personal Data Controllers must have a basis upon which Personal Data is processed–which is stipulated in 6 points: valid consent from the Personal Data Subject for several specific purposes, to fulfill obligations or request of an agreement, to fulfill legal obligations by the Personal Data Controller, to protect vital interests of the Personal Data Subject, to perform tasks within the scope of public interest or exercise authority, and to serve other legitimate interests with the purpose, needs, and balance between the Personal Data Controller and Personal Data Subject (Art.20(1)(2)).[53] Based on the consent for the processing of Personal Data under Article 20, it is stipulated in Article 21 that the Personal Data Controller must notify the legality of processing, purpose, type and relevance, retention period, detail of information collected, period of processing, Personal Data Subject Rights, and for any alteration of information to be notified by Personal Data Controller to the Personal Data Subject (Article 21). Moreover, Article 22, 23, 24, 28, and 29 goes into further detail in regards to the method of consent process which includes lawful data processing, data accuracy, and user

[52] Republic of Indonesia, Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection, Article 1(4)(5).

[53] Law No. 27 of 2022, Article 20(1)(2).

consent. Articles 25 and 26 are special Articles relating to obtaining consent for the processing of data of children and persons with disabilities whilst Article 27 stipulates how Personal Data Controllers must process Personal Data in a restricted, specific, lawful, and transparent manner.[54]

Taking into account every scenario in which data processing occurs, it is not possible for the law to cover every scenario, hence the layered safeguards present in the internal standard of procedure established by each controller and processor. These SOPs put into practice the principles of necessity, proportionality and risk mitigation. For example, whereas a hospital with elaborate health information should use the maximum security and exclusive consent measures, a simple health record system in a university can gain proportionate, less vigorous controls. Therefore, the two laws assign the technical how to the governance framework of each individual institution, and provide that sensitive data must always be given exceptional protection. According to data classification types on Sisa Fosec, data can be classified into three types; context-based, content-based, and user-based data. In the previously mentioned example, the sensitivity of data in both schools and hospitals can be classified as user-based and context-based data.[55] This also ties in to Article 21 of the PDP Law where it is stated that personal data can only be processed according to its purpose, type and relevance, and retention of data. Because schools would retain more general forms of health data due to its need of only requiring to know general data, there is less of a need to require technical ways to protect and treat the data whereas the data found in a hospital would be categorized as sensitive or special category of data due to its nature in order to protect the vital interests of the personal data subject (Art.20 PDP Law). Thus, this discusses the proportionality of consent requirements.

In terms of the controller and processor's responsibility, the GDPR is much more comprehensive and has a wider and more detailed scope

[54] Law No. 27 of 2022.

[55] SISA MKTG, "A Guide to Data Classification Types and Levels," SISA, 2020, https://www.sisainfosec.com/blogs/a-guide-to-data-classification-types-and-levels/.

and enforceability. Controllers and Processors can firstly defined in Article 4 (7) and (8) where the 'controller' refers to a natural or legal person which can determine the purpose and means of processing personal data, as according to regulation; whilst a 'processor' refers to a natural or legal person, public authority, or agency that processes data on behalf of the controller.[56] According to Article 5(2) of the GDPR, the data controller is responsible and must demonstrate compliance in accordance with how the personal data is to be processed–which is in a lawful, fair, and transparent manner.[57] Furthermore, these Articles are then reinforced in Article 24 where the principle of accountability is thus introduced, which mainly explains how controllers are required to not only comply, but must be able to demonstrate compliance alongside the obligations; states that data protection must be mandated by design and by default, which obligates controllers to integrate privacy safeguards to the data system. This brings Article 28–Processor–into the mix where in the case of processing being held out by a processor on behalf of the controller, they must be required to provide sufficient guarantees to implement appropriate privacy protection measures (Art. 28(1)).

Rights and obligations belonging to a Processor are written as the following: to not engage with another processor without prior permission from the controller and if it must be, the controller must be informed of any changes made (Art. 28(2)), processing must be governed under contract or under legal act which constitutes the scope, purpose, duration, and nature of the data processing, the rights, and responsibilities of the controller and processor. Such a contract has to provide that the processor performs based on the documented instructions by the controller, preserves confidentiality, takes adequate security measures under Article 32, and receives approval prior to involving another processor. The processor shall also support the controller with the rights to the data subject and compliance of Articles 32 to 36, delete or handover personal data on the pains of finishing the services unless required by law, and disclose all information necessary to

[56] Regulation (EU), Regulation (EU) 2016/679 (General Data Protection Regulation), Article 4(7)(8).

[57] Regulation (EU) 2016/679, Article 5(2).

show compliance such as allowing for audits. In addition, the processor should inform the controller in good time whenever it feels that any of its instructions go against the GDPR, or any other data protection law.[58] In addition to the following Articles, the regulation also imposes for the maintenance, processing and recording of activities to be kept under responsibility by the controller (Art.30), cooperation with supervisory authority (Art.31), the security of processing (Art.32), notification and communication of data breaches to the proper authorities as well as data subjects (Art.32 and 33), data protection impact assessments and prior consultation (Art.35 and 36), designations, position, and tasks of data protection officers (Art.37, 38, 39), and codes of conduct and certification (Art. 40, 41, 42, 43).[59]

Similarly to section 4.2.2, both the PDP Law and the GDPR are quite different in terms of their details and specifics in the controllers and processors rights and obligations. Both the PDP Law as well as the GDPR has established the roles of Data Controllers and Data Processors, however, the GDPR still provides a more comprehensive and detailed framework. As previously mentioned, Article 1(4–5) of the PDP Law is defined as, ".. an individual, a public body and an international organization that acts individually or collectively in order to define its purpose and control the processing of personal data. In the meantime, a Data Processor is a person who processes data on behalf of the Data Controller."[60]The definition provided by the GDPR can be found in Article 4(7-8) and Article 5(2), further expanding on the definition as well as providing clearer lines in terms of accountability and the responsibilities that the processor holds as subordinate to the controller. The GDPR elaborates further on how the processor is legally binding to the controller, hence mandating a binding legal contract with details on obligations such as confidentiality, processing, and the controller's instructions. The PDP Law in this scenario, could further improve the accuracy by giving the processors more accountability to take responsibility, as well as requiring a written or legal agreement that outlines all the rights obligations stated by the GDPR.

[58] Regulation (EU) 2016/679, Article 28 (1-10).
[59] Regulation (EU) 2016/679.
[60] Regulation (EU) 2016/679, Article 1(4)(5).

According to the the 'Comparative Review of Personal Data Protection Policy in Indonesia and The European Union's General Data Protection Regulation' written by Valentina Ancillia Simbolon and Vishnu Juwono, the fundamental difference of processing personal data in the GDPR is that it must go through a Data Protection Impact Assessment (DPIA) whereas PDP Law has no mention of any kind of assessment processes from the personal data protection authorities.[61] The author further explains that the GDPR's controllers and processors are obliged to take proactive accountability measures to ensure that the data processing activities are done responsibly and transparently. This involves conducting DPIAs, as previously mentioned, to identify and mitigate any potential risks that may occur to data subjects–prior to any processing taking place, as required under Articles 35 and 36 of the GDPR. Meanwhile, in Indonesia's PDP Law, while controllers and processors are referred to from Article 19–27, the law is more about having proper consent and lawful processing, and does not have a structured framework for risk analyses and monitoring for compliance. The GDPR is prohibitive by default, for instance, the special-category data processing is not permitted without a justification concerning Article 9(2), which guarantees maximum protection at the very beginning. On the other hand, the PDP Law is trigger based: special-data processing is authorized but claims other procedural protections in Articles 34–39, including the impact assessment of data protection and confidentiality responsibilities. This difference indicates the preventative policy of the GDPR in contrast to the conditional, risk-reducing policy of Indonesia.

As Simbolon and Juwono pointed out, the GDPR is more preventive and systematic in the fact that controllers have to not only gain consent but must also prove compliance along with GDPR data protection principles, through checks and documentation (Art. 5(2) and 24 GDPR).[62] In comparison, the PDP Law is still mostly declaratory as it lays out general obligations without providing any operational standards for the data controller and mandatory contractual

[61] Simbolon and Juwono, "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation."

[62] Simbolon and Juwono.

commitments for the processors, as stipulated in Article 28(3) GDPR. Ultimately, the GDPR and the PDP Law both lead towards the same end goal, namely the need to provide a layered protection to all personal data, both general and sensitive, through lawful, fair, and transparent processing. As previously stated, the GDPR implements safeguards using a prohibitive-rights framework based on accountability and prevention, whilst Indonesia uses a trigger-based or reaction-based framework based on a risk-assessment and procedural-compliance approach.[63] Controllers and processors in both systems have the main responsibility of using their utmost effort to achieve these standards and ensure that their internal processes, consent procedures, and data-handling processes comply with the regulations of each regime.

E. The Determinants of Valid Consent for Sensitive Data Collected by AI Chatbot

1. Challenges of Consent in AI Chatbot Use

There is a saying that parents would often tell their children every time they use the internet–that the internet is a jungle full of unknown dangers. For as long as the web has existed, it is most commonly known for people to always be careful when releasing personal and sensitive information unto the net, with reasons such as safety and non-disclosure of private information to any third parties with the fear of misuse of information. Yet in the age of Artificial Intelligence, in particular with the widespread use of AI chatbots, there is a new level of urgency in relation to precaution.

The implementation of the data processing (DP) principles in the context of the AI chatbots has brought in a difficult set of challenges related to consent and protection of personal data. As analyzed in accordance with Stanford's Module on Defining AI and Chatbots, AI Chatbot can be an interactive software application that is built from large language models (LLMs) that are designed to process, analyze, and generate human-like responses through the constant feeding of prompts

[63] Jing Yang, Yen-Lin Chen, Lip Yee Por, and Chin Soon Ku, "A Systematic Literature Review of Information Security in Chatbots," Applied Sciences 13, no. 11 (2023): 6355, https://doi.org/10.3390/app13116355.

and other data by users.[64] These chatbots can be not only be utilized in the case of some simple questions like on a Google Search, but a place to share personal thoughts and opinions, or the sharing of sensitive documents, which can be discussed or analyzed, without understanding that every single input can be stored, processed, and utilized to develop AI models further.[65] The issue lies in the fact that such personal or sensitive information after being provided to the system, gets into an automated system without the direct or immediate awareness or supervision of the user. This gives the very important question of what becomes of that data later: Who processes it? How long is it stored? Will it or can it ever be erased? This problem reveals the clash between the laws on protection of data, where personal data subjects need to explicitly and freely give consent (and the consent must be informed), and the work of AI chatbots, which tend to automate or blur the consent process. Although the GDPR and the PDP Law both provide legal grounds on gaining valid consent, the automated–processing of the AI systems poses a large danger towards issues of consent.

2. *The Nature of Consent in Automated Processing*

Automated–processing can be defined as technology that automatically handles the collection, transformation, analysis of data in large volumes and minimal human involvement.[66] Because manual handling is quite limited, automated processing reduces the errors that humans often make, where they can handle data with consistency and accuracy. Software tools that handle specific tasks such as data collection or algorithms that identify patterns in social media, are all examples of

[64] Defining AI and Chatbots," Stanford Teaching Commons, Stanford University, n.d., accessed November 29, 2025, https://teachingcommons.stanford.edu/teaching-guides/artificial-intelligence-teaching-guide/defining-ai-and-chatbots.

[65] Anna Leschanowsky, Silas Rech, Birgit Popp, and Tom Bäckström, "Evaluating Privacy, Security, and Trust Perceptions in Conversational AI: A Systematic Review," Computers in Human Behavior 159 (2024): 108344, https://doi.org/10.1016/j.chb.2024.108344.

[66] Mika Roivainen, "Automated Data Processing: Definition and Examples," 2025, https://www.esystems.fi/en/blog/automated-data-processing-definition-and-examples.

automated-processing. When applied within automated AI systems like chatbots, consent can be considered to have different definitions or requirements. In the data protection framework/regulations, consent must be provided freely, precisely, informed, and clear, as provided in Article 4(11) and Article 7 of the GDPR and in Article 20 of the PDP Law. However, in automated data processing, the process of consent is described to be handing over the reins of freedom of choice and control to data subjects, hence if the individuals do not have a real choice, consent is not freely given and would thus be invalid.[67] This connects to the topic of how users interact with chatbots by uploading personal documents or making use of such chatbots to divulge personal and private information without knowing how this data will be used, processed, or retained.

There is a common belief that a user's consent can be "assumed" because they continue to use the services of a website, stay silent, or don't untick a checkbox. In reality, there is a difference between explicit/informed consent, implied consent, and implicit participation. According to the GDPR, it is required for consent to be freely given, specific, and informed–hence consent being explicit through the full knowledge of what the data subject is agreeing to (Article 4(11) and Article 7). Explicit consent can also be considered as a higher bar in order to obtain access to special forms of data such as special categories of data (GDPR) or specific personal data (PDP Law). However, for ordinary personal data, consent is still considered to be unambiguous.[68] On the contrary of explicit consent, implied consent is consent that can be "assumed" through behaviours such as continuing to browse or use the services of a website, in this case AI Chatbots, not ticking an opt-out box, or staying silent after a notice. It is certainly offside to use "user didn't say no" as an argument, since the GDPR strictly states how consent should be an informed choice. In contrast to human-mediated consent in which the information is explicitly communicated, and the understanding of the data subject can be checked in-person, whilst

[67] ICO, "What Is Valid Consent?," 2025, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/.

[68] Alex Solo, "GDPR 'Implied' Consent – Why Guesswork Spells Trouble," Sprintlaw, 2025, https://sprintlaw.co.uk/articles/gdpr-implied-consent-why-guesswork-spells-trouble/.

automated systems receive "consent" through implied behavioural actions. This leads to a situation whereby the users are technically consenting to the collection of certain data without knowing the scope and consequences of it. In addition to that, personal data controllers must prove that any consent given by the data subjects was expressed in a clear and affirmative manner, and that the user reserves the right to revoke consent–under the GDPR (Article 7(3)). Similarly, the PDP Law states in Article 35, providing the right to revoke and the duty to stop the processing of data, in case a withdrawal is made. But in reality, the automation of consent in AI-related environments tends to undermine these protections. Because AI chatbots continue to collect and process data automatically, even without gaining the user's informed consent, users are repeatedly exposed to digital consent required in everyday life. Whether they come across a website to accept cookies or to read and accept lengthy Terms of Services notifications, users stop paying attention to what they agree to. This leads to 'consent fatigue', where users technically consent to a notification or requirement to access a service or website online, they are however not fully informed of the consequences of consenting.[69] Even though the consent is gained, it is not formally obtained with full information, thus making it not truly informed or autonomous.

Sebastian from the "Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information" journal describes how privacy notices in modern AI services are often long, wordy, and legalistic in nature and not read or comprehensible by the majority, which contributes to the situation where consent is made not meaningful but procedural.[70] The author explains that AI chatbots make this situation worse since the communication is two-way and ongoing-every reply, uploaded document or self-disclosure contributes to the system itself. The formal obligation of an informed consent is broken when users get used to the idea that they can become used to clicking

[69] Secure Privacy Team, "Adaptive Consent Frequency: Using AI to Combat Consent Fatigue," 2025, https://secureprivacy.ai/.

[70] Glorin Sebastian, "Privacy and Data Protection in Chatgpt and Other Ai Chatbots: Strategies for Securing User Information," *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)* 15, no. 1 (2023): 1–14, https://doi.org/10.4018/IJSPPC.325475.

on the notices or even using the chatbot without giving much thought to the consequences behind the data processing. This is in line with the notion that users are getting psychologically overloaded: they are being prompted to make privacy choices every single time, but the system is designed in such a way that the user is pressured to make a choice in favor of compliance due to the convenience and habituation. In the long run, this will create an erosion of attentiveness, a major indication of consent fatigue. It is also observed in "Data Protection and Privacy in the Age of Intelligent Machines", that the contemporary intelligent systems lack transparency and are massive in scale that it is almost impossible to trace how their personal data is being used, re-used or repurposed. It is highlighted in the text that the technical intricacy of automated processing is an immediate cause of disengagement in the users: when presented with unclear explanations, vague promises, or a heavy language of policy, people are not able to assess the risk in any meaningful way.[71] This is the key to consent fatigue: the repetition of prompts to consent, the absence of transparency and users choosing to trust or rely on convenience. This has drastic implications in AI contexts like chatbots, where data can be utilized to create training and improvement, profiling, or unpredictable downstream applications. Users can share information which is very personal with the belief that they are having a one-on-one interaction, yet there is no informed consent involved in reality.

To prevent explicit consent from becoming a mere legal formality, the Indonesian PDP Authority must address the architectural manipulation inherent in AI interfaces.[72] Consent fatigue, exacerbated by 'dark patterns'—such as pre-ticked boxes, confusing double negatives, or obscured opt-out paths—effectively nullifies the 'freely

[71] Dimitra Kamarinou et al., "Machine Learning with Personal Data," in *Data Protection and Privacy: The Age of Intelligent Machines* (Hart Publishing Oxford, 2017), 89–114, https://dokumen.pub/data-protection-and-privacy-the-age-of-intelligent-machines-9781509919345-9781509919376-9781509919352.html.

[72] Mourad Benseghir, Aouatef Zerara, Maamar Bentria, Halima Bendriss, and Mohamad Hidayat Muhtar, "Legal Aspects of Patient Data Governance in Digital Health: A Comparative Analytical Study of UAE and Indonesian Legislation," Journal of Indonesian Legal Studies 10, no. 2 (2025): 773–808, https://doi.org/10.15294/jils.v10i2.10025

given' and 'specific' requirements of the PDP Law. Therefore, the regulatory focus must shift from textual compliance to Privacy-by-Design standards.

3. *The Dangers of Automated Processing and Consequences*

One of the concerns of automated-processing comes with the training of data and its data retention. If the AI chatbot system makes use of data inputted into the software in order to make decisions and complex choices, there may be a risk of the data being re-purposed. This type of data would be invaluable to data brokers as the data from each individual would reveal insights into their behaviour–learning their preferences, identifying and profiling who they are and what they do, which would for instance, be valuable data for companies to maximize their effectiveness in the advertisement of campaigns or targeted ads.[73] In the event of an AI chatbot data breach, where the personal data of every individual is retained and kept in the system, these user's personal data could potentially be exposed and misused. A cybersecurity company, Group–IB from Singapore was discovered to have 101,100 devices infected with malware, making it possible to save ChatGPT login data. The following data was then found to be collected and sold and traded on dark web marketplaces. For instance, a high concentration of ChatGPT account data (exactly 26,802 in May 2023) were offered for sale over the past year.[74] In addition to that, employees within organizations have started using ChatGPT whether it is for software development or business communication, potentially exposing confidential or sensitive information which can be exploited to attack companies and its employees. The fact that 101,000 ChatGPT Accounts were stolen and sold on the dark web markets shows a clear poor handling of safeguarding user's chat history and data, which

[73] Adam John Andreotta and Björn Lundgren, "Automated Informed Consent," *Big Data & Society* 11, no. 4 (October 18, 2024): 20539517241289440, https://doi.org/10.1177/20539517241289439.

[74] GROUP-IB, "Group-IB Discovers 100K+ Compromised ChatGPT Accounts on Dark Web Marketplaces; Asia-Pacific Region Tops the List."

includes sensitive personal information.[75] The theft in the case demonstrates the dangers of improper handling of user subjects' personal data–especially if individuals are unaware of the proper consent mechanisms.

These info-stealing malware managed to harvest the credentials or data stored, allowing the stealers to pick up saved login information, browser cookies, bank card details, browsing history, and even other information from browsers. Because ChatGPT, by default, retains users' chat history, means that there will always be a risk of exposing private or sensitive content stored by the users. These are the security measures that come from stored communications and user data. As written by Martin Hasal on Chatbots: Security, privacy, data protection, and social aspects, communication is considered to be an extremely valuable asset, and many companies store past communications. The chatbot itself, from a general perspective, would record and learn how the user speaks from previous communication, in which they would copy the user's words, phrases, and random utterances in future conversations.[76] Apart from communication datasets such as these, which are hard to track, there are other concerns in regards to chatbot security that includes: cookies used on Webpages are known to save user activity such as chatbots which can subsequently be compiled or transferred to third parties. Chatbots usually retrieve usage information including button clicks, search queries, and patterns of interaction, which also may be sent out of the organization. Certain systems even permit the identification information, like names, email address, or device IDs, to be transferred, especially when the chatbot must take actions beyond its interface. Most chatbots use third-party messaging services that use their own terms and data-processing policies, such that a conversation can be logged or run off the user's knowledge. Lastly, we have the threat of conversational bias and manipulation: some social bots are actually designed to manipulate opinions, sell products, alter political opinion,

[75] Julia Ive, Vishal Yadav, Mariia Ignashina, Matthew Rand, and Paulina Bondaronek, "Privacy-Preserving Behaviour of Chatbot Users: Steering Through Trust Dynamics," arXiv preprint, 26 Nov 2024, arXiv:2411.17589.

[76] Martin Hasal et al., "Chatbots: Security, Privacy, Data Protection, and Social Aspects," *Concurrency and Computation: Practice and Experience* 33, no. 19 (October 10, 2021): e6426, https://doi.org/10.1002/cpe.6426.

or fake information. Such malicious bots are able to harm much because of their ability to mislead people and influence masses.[77]

Not only that but a case in March 2023 was reported by BBC about how ChatGPT leaked users' conversation histories due to a bug in the system. Some ChatGPT users could even view conversation titles that did not belong to them, including claiming on how they could see other user's chat histories and conversation.[78] According to BBC, OpenAI disabled ChatGPT for a few hours in order to fix the following error. This case also raises many issues of privacy and concern of ChatGPT's security measures.

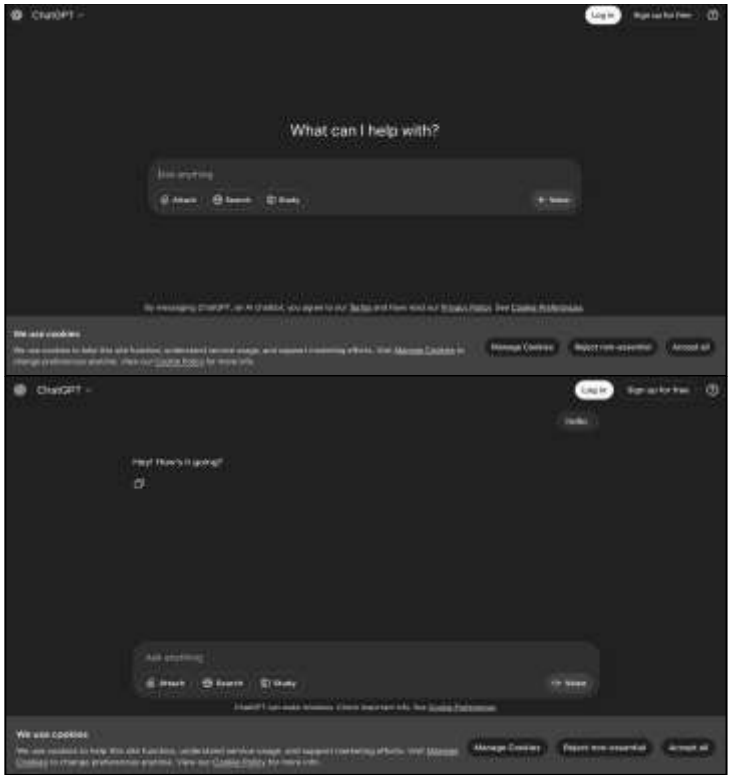

FIGURE 1. The standard page for users, when first logging into ChatGPT

[77] Hasal et al.

[78] Ben Derico, "ChatGPT Bug Leaked Users' Conversation Histories," BBC News, 2023, https://www.bbc.com/news/technology-65047304.

One of the dangers posed by automated consent is the manipulative use of dark-pattern interfaces that coerces a user into giving their consent without understanding the extent of their data processing as is often seen with large-language-model chatbots, in which a consent prompt is usually hidden behind a general terms-of-service banner, disappearing the moment the user starts interacting.[79] This example can be seen in Figure 1 where the chatbot has a dark-pattern interface with minimal text. Even the font for the warning on agreeing automatically to the terms and services as well as ChatGPT's privacy policy is written in small plain text, situated almost at the bottom of the page. It is easy for users to miss the message since the text appears to be not eye-catching. In the case of ChatGPT, once the user clicks on the textbox and uses the service by sending a message, the warning of agreeing to terms and services disappears, as can be seen in Figure 1. Additionally, the GDPR and PDP Law even states that valid consent must be freely given, specific, informative, and has clear purposes in the case of data processing. It can be seen from ChatGPT's interface that it does not employ proper consent mechanisms in accordance with the GDPR or even PDP Law's regulation. Companies should introduce an option for users to accept and willingly provide their personal data to be retained and processed by companies, by providing an "opt-in" option instead of an "opt-out" option, turning the process into a voluntary action.[80]

With that being said, in order to properly assess and place limits on automated-processing, knowing who is in charge and the responsibilities that befall the accountable, are essential for the future development and protection of personal data in AI Chatbots.

---

[79] Daniel Susser, Beate Roessler, and Helen Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World," *Georgetown Law Technology Review* 4 (2019): 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006.

[80] Glorin Sebastian, "Privacy and Data Protection in ChatGPT and Other AI Chatbots: Strategies for Securing User Information," *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)* 15, no. 1 (2023): 1–14; also available via SSRN, https://doi.org/10.2139/ssrn.4454761.

4. *Accountability of Personal Data Controllers, Personal Data Processors, and AI Developers*

Elayne Ruane states that developers must always strive to protect the personal integrity of a system's users. This is especially so in data protection and the particular concern in the development of conversational agents like ChatGPT.[81] This is because of the AI Chatbots familiar and friendly dialogue design that would lead to the users sharing their personal information. Therefore, every AI developer must be aware of all the difficulties befalling any type of data collection.

According to Linda Meyer, developers of AI Chatbots have ethical responsibilities when it comes to chatbot development. It is important to highlight important areas such as its reliability, relativization, and UI-design. Additionally, it is essential to maintain a certain level of awareness of the purpose of the creation of a chatbot.[82] The chatbot, aimed at responding to medical questions, should adhere to various ethical standards as compared to one that is used for customer service. Nonetheless, there exist certain broad-based ethics. The developers must safeguard the personal integrity and information of the chatbot users. Moreover, the software is also to be updated on the existing national laws and rules. Transparency is also another factor that should be considered, yet not everyone is convinced that it would eliminate the issue of moral authority of ChatGPT completely. However, the use of a chatbot must tell users of its limitations. Lastly, it is evident that new studies should be conducted in the future that will provide developers with more guidelines that would facilitate ethical development of chatbots. This can be explained by the fact that chatbots are used in different fields, including health care and education.

Therefore, chatbot developers must be subject to GDPR regulations, where data protection by lawfulness, fairness and transparency will be the major factor in the personal data that is stored.

---

[81] Elayne Ruane, Abeba Birhane, and Anthony Ventresque, "Conversational AI: Social and Ethical Considerations.," *The Irish Software Research Centre* 2563 (2019): 104–15, https://ceur-ws.org/Vol-2563/aics_12.pdf.

[82] Linda Meyer, "ChatGPT and the Developer's Ethical Responsibility: A Literature Study of Chatbot-Related Ethical Dilemmas from the Developer's Perspective" (Thesis, Sweden: Linnaeus University, Faculty of Technology, Department of computer science and media technology (CM), 2023).

To be in compliance with the laws and regulation, it is also required for the personal data to be accurate, the rights of individuals to be balanced with those of the organizations, the confidentiality of the data to be guaranteed and the data retention time to be limited, thus, minimizing the risk of potential security threats.[83] In detail, according to the GDPR, Article 32(a) requires companies to take measures like anonymization and encryption of personal data. Communication data with a chatbot may be kept, but must not have any link to an individual user and his or her data, and it must be secure. In the first case, the database consists of only communication data and is allowed to be accessed by the development staff; however, it must not contain any information that can identify a person either directly or indirectly.

Aside from the already-present responsibilities that come with the development and management of AI Chatbots, another important factor is in fact–the users themselves and how they use AI Chatbots.

The journal, 'Code' and the Slow Erosion of Privacy' discusses the side-effect of technological development being a gradual erosion of privacy. It explains that this erosion of privacy is a natural process that comes with the gradual evolution of technology, and how individuals in a society also gradually adapt themselves to the possibilities of sharing and monitoring more information instead of shielding.[84] The expectations of privacy slowly change with technological evolution. As quoted from Michael Froomkin, in accordance with the journal, "Looking back and clinging to privacy protection may be old-fashioned when we observe youngsters leaving massive data trails on the Internet and chatting intimidate details into mobile phones in public, without regard for potential privacy effects."[85] This quote clearly explains a pressing issue in today's digital age, where individuals set aside privacy for exposure, continuing to release personal and private content of themselves onto the internet. This same issue prevails in a previously

[83] Hasal et al., "Chatbots: Security, Privacy, Data Protection, and Social Aspects."

[84] Bert-Jaap Koops and Ronald Leenes, "Code and the Slow Erosion of Privacy," *Michigan Telecommunications and Technology Law Review* 12, no. 1 (2019): 115, https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1114&context=mttlr.

[85] Susser, Roessler, and Nissenbaum, "Online Manipulation: Hidden Influences in a Digital World."

discussed concept of AI Chatbot users making use of ChatGPT as a tool for personal confiding or a place to pour out personal information about themselves, sometimes even going as far as providing advice and acting as therapists to users.

Because of the existence of AI Chatbots now, many users have discovered a new outlet that doesn't require the need to actually interact with another person, but being able to converse in-depth, with the AI as if it were a therapist or a close friend. It is understandable why AI is more appealing to users who frequent online platforms; it is readily available, accessible at all times and much cheaper than the usual ways of receiving mental health care like therapists. However, this doesn't mean that users can send whatever they wish into AI Chatbots because ultimately, the users themselves should also be responsible for inputting data into AI Chatbots. Users of AI Chatbots must learn to take responsibility for what they input into chatbots as well, including any kind of information that hints at more specific and special categories of information. According to Linda Meyer, users may still disclose his or her data unintentionally. And because data can be learned and inferred from a conversation, the user may not be aware that they are sharing sensitive information with an AI Chatbot.[86]

5. *Pathways for Safer and more Lawful AI Chatbot Use*

The challenges and issues found in current AI Chatbot consent validity, gives a chance of reconsidering the way conversational AI could be designed, regulated, and implemented in a way that does not violate legal provisions or rights of users. Instead of only focusing on shortcomings and gaps in liability in terms of automation, it is also essential to identify pathways with opportunities to improve AI Chatbot use to be safer and more lawful, in hopes to reduce risks when operating AI Chatbots. The following pathway focuses on involving and enhancing the transparency and understanding provided by the users through better conversational-consent processes, redesigning chatbot interfaces to enable explicit and informed permission, embracing ethical AI principles to be responsible in processing data, and predicting future

[86] Meyer, "ChatGPT and the Developer's Ethical Responsibility: A Literature Study of Chatbot-Related Ethical Dilemmas from the Developer's Perspective."

regulatory or technical remedies that would enhance the integrity of consent. A thorough analysis of these strategies could offer a balanced overview of how AI systems could develop to be more compliant, accountable, and secure for user personal data.

Transparency is an important cornerstone when it comes to trust. As stated in Emmanuel's thesis, the concept of transparency implies that the users must know the system functionality such as its data sources, decision-making models, and constraints. This includes the explicit announcement of the mode of the chatbot (rule-based or machine-learning-driven), clarity on the data that it uses, and clarifications on how it produces responses.[87] In the meantime, transparency should be further enhanced through different ways. One of the ways could be clearly informing users that they are interacting and communicating with an AI system, providing feedback to users and giving users the freedom to choose their preferred settings as well as data collection preferences.[88] In this way, chatbots would be assisting users by allowing them to make more informed decisions and have a freedom of choice by embedding these transparency practices into AI conversational-consent flows, thus helping users realize the consequences of providing personal data. AI Chatbots should come with clear warnings instead of just a blank screen, as dictated by Figure 1.

Another pathway is to introduce more transparent regulatory and technical protection in favor of legal consent. As observed by Beauden, AI governance should be a shared responsibility between governments, the industry, and researchers in order to develop frameworks, including the newly developed EU AI Act, that directly governs the use of AI and prevent abuse. This involves setting up independent audits and certifications to check the fairness, accuracy and ethical compliance of chatbot systems.[89] Combined with this, Emmanuel also emphasizes that

---

87 Emmanuel Ok, "Transparency and Explainability in AI Chatbots: How They Shape User Confidence" (Thesis, Ogbomoso: Ladoke Akintola University of Technology, Department of Computer Science and Engineering, 2025).

88 Beauden John, "User Perceptions of AI Chatbots: Analyzing Fear, Skepticism, and Acceptance," ResearchGate, 2025, https://www.researchgate.net/publication/389283323_User_Perceptions_of_AI_Chatbots_Analyzing_Fear_Skepticism_and_Acceptance.

89 John.

AI chatbots should be regularly audited and updated in terms of transparency and maintain their continuity to the standards, including GDPR and ethical AI principles. Such audits enable the developers to constantly perform bias tests, judge fairness, and determine whether the data practices remain respectful of user rights. Beauden and Emmanuel agree with the existence of audits for AI companies. Audits could perhaps be done in the form of a commission or a government and independent commission that audits the practices a company applies, in order to safeguard data. Auditing may extract a great deal of resources and trust, however, it could keep AI companies 'on their toes', so they cannot do whatever they please with users' personal data.

In addition to technical reviews, in terms of regulatory oversight, shortcomings of the Indonesian PDP Law in mitigating risks posed by automated-processing are largely due to its absence of prescriptive regulatory guidelines and its strong dependence on the will of individual data controllers. Contrasting the GDPR, which requires the introduction of the structured protection of the DPIAs, by Articles 34 and 35, the PDP Law lacks minimum guidelines to establish the possible harm or degree of risk in data processing operations. This regulatory failure as indicated in Jovan Rafael's thesis, leads to subjective and inconsistent risk interpretation that enables each controller to set his or her own standards according to internal capacity in lieu of a definite threshold as stipulated by law.[90] Lack of harmonized requirements implies that protections differ in sectors creating unequal protection levels, which is disastrous in automated systems that handle data in torrents and at unprecedented levels. Moreover, the PDP Law also moves most of the technical and organizational protection to institutions without a more thorough guideline, which is why the analysis of harm within AI-based environments, where profiling, inference, or repurposing of data can proceed without user authority, is not adequately examined. All these gaps show that the PDP Law is still unprepared to solve the systemic risks and obscurity of automated-

[90] Jovan Rafael Aurelio Susento, "Perbandingan Hukum Peraturan Pelindungan Data Pribadi Indonesia Dengan Uni-Eropa Mengenai Kebocoran Data Pribadi Lingkup Instansi Pemerintahan" (Thesis, Jakarta: Program Studi Hukum Fakultas Hukum Universitas Pelita Harapan, 2024).

processing, and thus placing the personal data subjects at risk. Additionally, both the GDPR and the PDP Law will not always have the power to catch-up to AI's technological advances completely, making some regulations quickly outdated. The existing legislations, may for instance, look at *ratio legis* of the OECD privacy principles, of which its aim is to reconcile the freedom of information flow with the basic right to privacy, foster trust among nations, and avert abuse of personal information, and inform the creation of domestic privacy legislation.[91] Due to the fact that AI systems frequently process data beyond what users understand or consents to, the GDPR and the PDP Law are increasingly finding new obstacles when upholding objectives such as these.

Another issue brought by Linda Meyer comes to light, in which "Regulations such as the GDPR strictly define data manipulation methods, but not everybody lives in the EU under the jurisdiction of GDPR regulations for data protection. All personal information should be deleted from such data in the EU, but it is almost impossible to check if this is true." This indicates a larger issue in terms of data protection around the world. Even with laws and regulations such as the GDPR put into place, it is difficult to implement and enforce the laws if there is no "sovereign". Data protection regulations in different countries would obviously vary, thus making it difficult to implement and monitor compliance. Bert-Jaap Koops and Ronald Leenes suggest the question of a sovereign in AI regulations–or a set of rules placed worldwide to govern AI systems. The authors suggest that the main challenge of controlling automated-processing and AI, are the rule-makers of the digital space instead of politicians, also known as the programmers who code the AI system.[92] Even though the developers are not lawmakers, the choices they make in a technical sense, inadvertently creates a system to either secure or eliminate privacy. Even minor design decisions such as the recording data, where it is saved or encrypted can slowly erode privacy, a phenomenon known as a slow erosion of privacy, according to Ronald Leenes. By doing so, developers are made *de facto*

[91] Fajar Sugianto, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; An Overview*, *Slide Show*, 2025.

[92] Koops and Leenes, "Code and the Slow Erosion of Privacy."

authorities whose technical decisions have regulatory implications even without any intent to do so. In the case of privacy-enhancing technologies (PETs), 'power' is transferred to the creators of the technology. Such developers can be affected by Data Protection Authorities, privacy advocacy groups or even government agencies. This implies that the distribution of power becomes unstable in the setting of automated-processing, where developers create the systems according to which data flows are organized, and governments openly or covertly interfere with it.[93] Consequently, meaningful privacy and valid consent in AI systems becomes challenging to guarantee, since those involved in the process of creating the systems are not necessarily in compliance with the law, user expectations, and moral standards. The more data a company has, the more favourability the user would have. On the whole, these problems indicate that it is extremely complicated to regulate AI and automated-processing. Power is shared among the states, the private developers and the technical design of the code itself. Unless the world is united in its efforts, the GDPR, as well as the PDP Law, will not be able to ensure that personal information is not violated, since the actual authority over data can be outside of any single legal framework.

The design and development of AI systems should be structured to build ethical values so as to reinforce the validity of consent. Algorithms bias, privacy breaches, manipulative interface design, and deceitful user experiences are some of the ethical risks that may severely threaten user autonomy and corrupt the procedure of consent.[94] To mitigate these issues, building ethical AI processes should become a consistent priority by developers that includes the inclusion of bias identification and alleviation, effective data-protection protocols like encryption and anonymisation, and precautionary actions against

[93] Firsta Rahadatul 'Aisy, Muhammad Azil Maskur, and A.M. Adzkiya' Amiruddin, "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore," Journal of Indonesian Legal Studies 10, no. 1 (2025): 431–482, https://doi.org/10.15294/jils.v10i2.10025

[94] Karishma Verma, "Digital Deception: The Impact of Deepfakes on Privacy Rights," Lex Scientia Law Review 8, no. 2 (December 2024): 859–896, https://doi.org/10.15294/lslr.v8i2.13749

manipulative dialogue methods. It is also significant to define a good accountability framework among developers and system operators. With further explanations by Emmanuel, the ethical AI must be evaluated by way of feedback loops, system updates, and compliance assessments to make sure that the technology becomes adjustive to the set ethical standards.[95] A combination of these principles will facilitate the development of chatbot systems that will actually adhere to the rights of users, minimize the likelihood of coercion or misleading communication, and make consent not only a mandatory but substantively meaningful process.

Lastly, a further legalized application of AI chatbots implies that design decisions directly affecting the method of seeking and grasping consent need to be reconsidered. Such transparency characteristics as the explicit identification of the chatbot as an AI system and explanatory design of its answers should be integrated into the user interface, so that it would not be misleading or manipulative.[96] This can be reinforced through increased user control settings wherein one can choose not to be collected or have privacy settings. This is supported by Emmanuel as well, where it emphasizes the need of user control, integration of feedback and clarity of data-source in the general system architecture. Combined, these design enhancements can facilitate the development of conversational-consent pathways to act as an ongoing process of interactivity, ongoing and comprehensible, as opposed to one passive click-through. The developers can more easily comply with the legal and ethical standards of valid consent through the creation of clear chatbot interfaces that define the purpose of data usage and are free of manipulative elements.

AI chatbots do not necessarily mean any harm, but the risks arise from the legal framework and design choices that shape the way these systems gather, process, and store personal data. The validity of consent does not only depend on regulations such as the GDPR and PDP Law, however, other parties such as AI developers, interface designers,

[95] Ok, "Transparency and Explainability in AI Chatbots: How They Shape User Confidence."

[96] John, "User Perceptions of AI Chatbots: Analyzing Fear, Skepticism, and Acceptance."

platform operators, the company itself, depends on the technical and ethical decisions they make. At the end of the day, when there are proper legal safeguards present along with a transparent system design with responsible and responsible development practices, AI chatbots can be used in a way that does not violate the autonomy of users and does not compromise data protection principles. On the other hand, in case these elements are inefficient or inconsistent, the same technologies may harm informed consent and put customers at a risk of serious privacy harm.

F. Conclusion

The PDP Law does not have the means to regulate advancing technologies such as AI yet, creating gaps in legal certainty and enforcement. As such, the GDPR may serve as an example to strengthen and fill in regulatory gaps in the PDP Law. The PDP Law can be extended, specifically in its definition of the term 'specific personal data', and strengthen the rights and responsibilities of data subjects, controllers, and processors to become more accountable. Although both laws are similar in concept, the GDPR provides more specific and prescriptive requirements, such as rights to rectification, erasure, objection, and data portability, which are not operationalized in the PDP Law. This difference can also be demonstrated by the comparison of enforcement regimes: GDPR offers a system of administrative fines, corrective actions, and a single system of supervisory authority, whereas the PDP Law does not have such procedures, and the penalties are relatively less extensive. To conclude, both frameworks share the aim to safeguard general and sensitive personal data, but the GDPR is still much more specific, focused, and detailed.

In order to fully understand how to incorporate data protection and AI regulations into the PDP Law, it is essential to look into AI systems in practice–in this case, the AI Chatbot system. Due to the emergence of conversational AI Chatbot systems, the safety of a user's personal data gradually grows in risk. Many users tend to reveal personal and sensitive information about themselves into conversational chatbots–unaware that their data could be reused, stored, or learned by the system. The AI Chatbot systems can collect, retain, and process said personal and sensitive data. The big question was where the data goes

and whether these systems employ valid consent mechanisms, in particular due to the fact that most users tend to reveal personal information without an intention to do so. As such, accountability in AI systems was addressed through examining the responsibilities of data controllers, data processors, and AI developers–along with the responsibility of users themselves. It is then found that in order for all parties to ensure the safety of personal data: raising transparency and user awareness, remodeling chatbots to enable explicit and informed consent, integrating ethical AI principles like fairness and responsibility, and legislating the proper regulatory measures to combat the issue. These are necessary in order to achieve an AI chatbot system that upholds the rights to privacy and validity of consent, and not as a mere formality.

Based on the comparative success of the EU's approach, this research proposes three concrete recommendations for the Indonesian PDP Authority to establish standardized interface requirements. First, regulators should mandate a tiered disclosure system where AI chatbots must provide a clear, high-level summary of data processing activities (first layer) before prompting for detailed consent (second layer). This prevents information overload and ensures the user understands the core processing intent. Second, to combat dark patterns, the PDP Authority should issue guidelines requiring 'Accept' and 'Decline' options to be presented with equal visual prominence. The use of 'deceptive nudging'—where the 'Accept' button is highlighted while the 'Decline' option is hidden in sub-menus—must be classified as a violation of the explicit consent principle under the PDP Law. Third, given that AI models evolve through continuous training, consent should not be a one-time event. Regulators should require real-time notices—intermittent prompts that remind users when their sensitive emotional data is being used for model retraining—allowing users to withdraw consent specifically for secondary processing without losing access to the primary service.

G. References

Ademokun, Oluwatosin Victoria. "AI And the GDPR: Understanding the Foundations of Compliance." TechGDPR, 2025. techgdpr.com/blog/ai-and-the-gdpr-understanding-the-foundations-of-compliance.

Aisy, Firsta Rahadatul, Muhammad Azil Maskur, and A.M. Adzkiya' Amiruddin. "Establishing Indonesia's Personal Data Protection Agency: Comparative Administration Sanctions Enforcement from Ireland, Australia, and Singapore." *Journal of Indonesian Legal Studies* 10, no. 1 (2025): 431–482. https://doi.org/10.15294/jils.v10i2.10025.

Aminy, Yudhi PrasetyoReza. "Introduction of the Official Personal Data Protection Act (UU PDP)." BDO, 2024. https://www.bdo.co.id/en-gb/insights/introduction-of-the-official-personal-data-protection-act-(uu-pdp).

Andreotta, Adam John, and Björn Lundgren. "Automated Informed Consent." *Big Data & Society* 11, no. 4 (October 18, 2024): 20539517241289440. https://doi.org/10.1177/20539517241289439.

Asiean Breafing. "Indonesia's Comprehensive Personal Data Protection Law Guide - Indonesia Guide." Doing Business in Indonesia, 2025. https://www.aseanbriefing.com/doing-business-guide/indonesia/company-establishment/personal-data-protection-law.

Bagdasarian, Eugene, Ren Yi, Sahra Ghalebikesabi, Peter Kairouz, Marco Gruteser, Sewoong Oh, Borja Balle, and Daniel Ramage. "AirGapAgent: Protecting Privacy-Conscious Conversational Agents." In *Proceedings of the ACM Conference on Computer and Communications Security* (CCS '24), December 9–13, 2024. DOI:10.1145/3658644.3690350.

Benseghir, Mourad, Aouatef Zerara, Maamar Bentria, Halima Bendriss, and Mohamad Hidayat Muhtar. "Legal Aspects of Patient Data Governance in Digital Health: A Comparative Analytical Study of UAE and Indonesian Legislation." *Journal of Indonesian Legal Studies* 10, no. 2 (2025): 773–808.

https://doi.org/10.15294/jils.v10i2.10025

Burmagina, Kseniia. "ChatGPT Usage: Statistics and Facts." Elfsight, 2025. https://elfsight.com/blog/chatgpt-usage-statistics/.

Carmichael, Laurie, Sara-Maude Poirier, Constantinos K. Coursaris, Pierre-Majorique Léger, and Sylvain Sénécal. "Users' Information Disclosure Behaviors during Interactions with Chatbots: The Effect of Information Disclosure Nudges." *Applied Sciences* 12, no. 24 (2022): 12660. https://doi.org/10.3390/app122412660.

Chin-Rothmann, Caitlin. "Protecting Data Privacy as a Baseline for Responsible AI." Protecting Data Privacy as a Baseline for Responsible AI, 2024. https://www.csis.org/analysis/protecting-data-privacy-baseline-responsible-ai.

Derico, Ben. "ChatGPT Bug Leaked Users' Conversation Histories." BBC News, 2023. https://www.bbc.com/news/technology-65047304.

European Commission. "Data Protection Explained." European Commission, 2025. https://commission.europa.eu/law/law-topic/data-protection/data-protection-explained_en.

Exabeam. "The Intersection of GDPR and AI and 6 Compliance Best Practices." Exabeam, 2025. www.exabeam.com/explainers/gdpr-compliance/the-intersection-of-gdpr-and-ai-and-6-compliance-best-practices/.

General Data Protection Regulation (GDPR). "Consent - General Data Protection Regulation (GDPR)," 2024. https://gdpr-info.eu/issues/consent/.

GROUP-IB. "Group-IB Discovers 100K+ Compromised ChatGPT Accounts on Dark Web Marketplaces; Asia-Pacific Region Tops the List." GROUP-IB, 2023. www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials.

Gumusel, Ece. "A Literature Review of User Privacy Concerns in Conversational Chatbots: A Social Informatics Approach." *Journal of the Association for Information Science and Technology* 76, no. 1 (2024): 121–54. https://doi.org/10.1002/asi.24898.

Hasal, Martin, Jana Nowaková, Khalifa Ahmed Saghair, Hussam Abdulla, Václav Snášel, and Lidia Ogiela. "Chatbots: Security, Privacy, Data Protection, and Social Aspects." *Concurrency and Computation: Practice and Experience* 33, no. 19 (October 10,

2021): e6426. https://doi.org/10.1002/cpe.6426.
ICO. "A Guide to the Data Protection Principles." ICO, 2025. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/.
ICO. "What Is Valid Consent?," 2025. https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/consent/what-is-valid-consent/.
Ive, Julia, Vishal Yadav, Mariia Ignashina, Matthew Rand, and Paulina Bondaronek. "Privacy-Preserving Behaviour of Chatbot Users: Steering Through Trust Dynamics." arXiv preprint, 26 Nov 2024. arXiv:2411.17589.
John, Beauden. "User Perceptions of AI Chatbots: Analyzing Fear, Skepticism, and Acceptance." ResearchGate, 2025. https://www.researchgate.net/publication/389283323_User_Perceptions_of_AI_Chatbots_Analyzing_Fear_Skepticism_and_Acceptance.
Kamarinou, Dimitra, Christopher Millard, Jatinder Singh, and R Leenes. "Machine Learning with Personal Data." In *Data Protection and Privacy: The Age of Intelligent Machines*, 89–114. Hart Publishing Oxford, 2017. https://dokumen.pub/data-protection-and-privacy-the-age-of-intelligent-machines-9781509919345-9781509919376-9781509919352.html.
Koops, Bert-Jaap, and Ronald Leenes. "Code and the Slow Erosion of Privacy." *Michigan Telecommunications and Technology Law Review* 12, no. 1 (2019): 115. https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1114&context=mttlr.
Leschanowsky, Anna, Silas Rech, Birgit Popp, and Tom Bäckström. "Evaluating Privacy, Security, and Trust Perceptions in Conversational AI: A Systematic Review." *Computers in Human Behavior* 159 (2024): 108344. https://doi.org/10.1016/j.chb.2024.108344.
LII (Legal Information Institute). "Right to Privacy." LII, 2025.
Meyer, Linda. "ChatGPT and the Developer's Ethical Responsibility: A Literature Study of Chatbot-Related Ethical Dilemmas from the Developer's Perspective." Thesis, Sweden: Linnaeus University,

Faculty of Technology, Department of computer science and media technology (CM), 2023.

Neufeld-Wall Maya, and Trinity University. "Being Real: Gen-Z, Self-Presentation, and Authenticity on Social Media." Digital Commons @ Trinity, 2023. digitalcommons.trinity.edu/cgi/viewcontent.cgi?article=1026&context=comm_honors.

NewsGP. "Increase in Patients Turning to AI for Therapy." NewsGP, 2025. www1.racgp.org.au/newsgp/professional/increase-in-patients-turning-to-ai-for-therapy.

Ok, Emmanuel. "Transparency and Explainability in AI Chatbots: How They Shape User Confidence." Thesis, Ogbomoso: Ladoke Akintola University of Technology, Department of Computer Science and Engineering, 2025.

Pujianti, Sri. "Govt: Law on Personal Data Protection Provides Legal Protection." Constitutional Court of the Republic of Indonesia, 2023. https://en.mkri.id/news/details/2023-02-13/Govt:_Law_on_Personal_Data_Protection_Provides_Legal_Protection.

Regulation (EU). Regulation (EU) 2016/679 (General Data Protection Regulation) (2016).

Republic of Indonesia. Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (2022).

Roivainen, Mika. "Automated Data Processing: Definition and Examples," 2025. https://www.esystems.fi/en/blog/automated-data-processing-definition-and-examples.

Ruane, Elayne, Abeba Birhane, and Anthony Ventresque. "Conversational AI: Social and Ethical Considerations." *The Irish Software Research Centre* 2563 (2019): 104–15. https://ceur-ws.org/Vol-2563/aics_12.pdf.

Sebastian, Glorin. "Privacy and Data Protection in Chatgpt and Other Ai Chatbots: Strategies for Securing User Information." *International Journal of Security and Privacy in Pervasive Computing (IJSPPC)* 15, no. 1 (2023): 1–14. https://doi.org/10.4018/IJSPPC.325475.

Secure Privacy Team. "Adaptive Consent Frequency: Using AI to Combat Consent Fatigue," 2025. https://secureprivacy.ai/.

Simbolon, Valentina Ancillia, and Vishnu Juwono. "Comparative Review of Personal Data Protection Policy in Indonesia and the European Union General Data Protection Regulation." *Publik (Jurnal Ilmu Administrasi)* 11, no. 2 (2022): 178–90. https://doi.org/10.31314/pjia.11.2.178-190.2022.

SISA MKTG. "A Guide to Data Classification Types and Levels." SISA, 2020. https://www.sisainfosec.com/blogs/a-guide-to-data-classification-types-and-levels/.

Solo, Alex. "GDPR 'Implied' Consent – Why Guesswork Spells Trouble." Sprintlaw, 2025. https://sprintlaw.co.uk/articles/gdpr-implied-consent-why-guesswork-spells-trouble/.

Sugianto, Fajar. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; An Overview. Slide Show*, 2025.

Susento, Jovan Rafael Aurelio. "Perbandingan Hukum Peraturan Pelindungan Data Pribadi Indonesia Dengan Uni-Eropa Mengenai Kebocoran Data Pribadi Lingkup Instansi Pemerintahan." Thesis, Jakarta: Program Studi Hukum Fakultas Hukum Universitas Pelita Harapan, 2024.

Susser, Daniel, Beate Roessler, and Helen Nissenbaum. "Online Manipulation: Hidden Influences in a Digital World." *Georgetown Law Technology Review* 4 (2019): 1. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3306006.

Taufiq, Muchamad, and Ananda Salsabila Kenyo. "The Legal Protection of Personal Data in the Digital Era: A Comparative Study of Indonesian Law and the GDPR." *International Journal of Business, Law, and Education* 6, no. 2 (2025): 1260–68. http://ijble.com/index.php/journal/article/view/1178.

TermsFeed. "Personal Vs. Sensitive Personal Information." Termly, 2025. https://termly.io/resources/articles/sensitive-personal-information/.

United Nations - CEB. "Principles on Personal Data Protection and Privacy." United Nations - CEB, 2025. https://unsceb.org/principles-personal-data-protection-and-privacy-listing.

Verma, Karishma. "Digital Deception: The Impact of Deepfakes on Privacy Rights." *Lex Scientia Law Review* 8, no. 2 (December

2024): 859–896. https://doi.org/10.15294/lslr.v8i2.13749.

Witcher, Rob. "OECD Privacy Guidelines & Security | CISSP Study Guide." Destination Certification, 2025. https://destcert.com/resources/oecd-privacy-principles-global-security/.

Yang, Jing, Yen-Lin Chen, Lip Yee Por, and Chin Soon Ku. "A Systematic Literature Review of Information Security in Chatbots." *Applied Sciences* 13, no. 11 (2023): 6355. https://doi.org/10.3390/app13116355.

***

Privacy is not just about hiding things or keeping secret, it's about controlling who has access to your life.

Timsux Wales
A Cybersecurity Professional

Acknowledgment

The authors gratefully acknowledge the Faculty of Law, Universitas Pelita Harapan, for the institutional support and resources provided to conduct this research. We also extend our sincere appreciation to Ginzaseiwa Law Office for their valuable support and contribution to this study. Finally, the authors wish to recognize the dedicated collaborative effort and synergy among the research team that made the completion of this work possible.

Funding Information

None

Conflicting Interest Statement

The authors state that there is no conflict of interest in the publication of this article.

Publishing Ethical and Originality Statement

All authors declared that this work is original and has never been published in any form and in any media, nor is it under consideration for publication in any journal, and all sources cited in this work refer to the basic standards of scientific citation.

Generative AI Statement Statement

In the preparation of this manuscript, the authors employed Generative AI technologies exclusively for the purposes of language translation and the adaptation of research models. No original data or substantive content was generated by AI tools. The authors have reviewed and edited the output to ensure accuracy and take full responsibility for the integrity of the work.