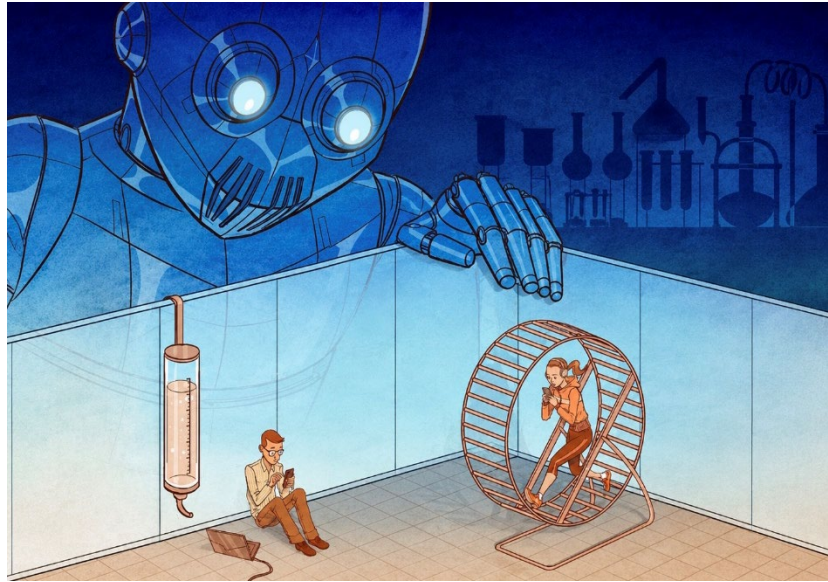


21st Century's Siren Song: How is Personal Data protected from the seduction of AI?

Man, completely unguarded, plunges headfirst into the rocks laid out by those who wield the power of AI... Will this be the inevitable tragedy that we are sailing towards?



Introduction

From the early “hey Siri!” to the current “Chat, please generate...”, smarter and more mainstream Artificial Intelligence (AI) bots have begun dominating the 21st century: AI has been deeply integrated into our online shopping experiences, designing our algorithm to recommend products according to our personalised preferences; AI has become many students’ go-to tutor, introducing them to new perspectives and helping them to solve problems; AI has even made its presence relevant in our healthcare, serving advisory roles to help users plan their meals and customise exercise regimes.¹ Building on their success, AI developers continue to fill our ears with the sweet promises of their creation, luring mankind aboard a vessel meticulously engineered from the information we readily surrender with just a few mindless clicks of our keyboards – only to end in shipwreck.

What is Personal Data?

Personal data is any information that enables a person to be distinctly identified. Such information includes names, contact numbers, email addresses, photographs, voice recordings, biometric information and financial records.²

¹“Does using ChatGPT for homework make kids lazy? Here’s my rule at home” CNA, Mar 14, 2026

²“AI-specific notifications mandatory for firms using personal data to train AI models: PDPC” The Straits Times, Jul 21, 2026

How do developers train their AI models?

Training AI models require countless rounds of feeding pertinent data into the model and adjusting the model's parameters to reduce the disparity between the model's predictions and the original data.³ These datasets will vary with the function of the model.⁴ For example, AI assistants used to provide financial advice will need to receive input information such as the age, annual income and spending habits of customers in order to generate sound and suitable recommendations. The more training data is available, the more AI models can be fine-tuned to better provide the services they are deployed for.

What dangers do AI training expose us to?

By default, every prompt we enter into these chatbots is retained in the AI system for training.⁵ From a study conducted at Swiss university ETH Zurich in 2014, researchers found that AI chatbots are capable of building rich, granular profiles of its users based on past conversations with an accuracy of up to 85%.⁶ Since then, these models have advanced significantly.

This can become problematic because the abundance of personal data stored in these systems pose a very real risk of exploitation, which can lead to modern forms of slavery. Pope Leo XVI illustrates this dystopian reality in his Encyclical *Magnifica Humanitas* as such⁷: "Those who control the health data of entire peoples — often collected under the pretext of aid, research or innovation — possess a structural leverage over the future, for they can shape needs and markets. They can also decide, before others, to whom medicines, investments and protections will be allocated." In this way, consumers are reduced to pawns under the control of organisations, completely stripping people off the human dignity that we so firmly champion for in today's world.

New Advisory Guidelines on Use of Personal Data in Generative AI ("GenAI")

During the recent Singapore Data Festival 2026, the Personal Data Protection Commission ("PDPC") announced new regulations governing the collection and use of personal data by organisations.⁸

³"How generative A.I. really works" The New York Times, May 5, 2023

⁴"ST Explains: When must firms inform customers about using their personal data for AI training?" The Straits Times, July 21, 2026

⁵Be Careful What You Tell Your AI Chatbot (Oct 15, 2025). Stanford University Human-Centred Artificial Intelligence. <https://hai.stanford.edu/news/be-careful-what-you-tell-your-ai-chatbot>

⁶"AI chatbots know more about you than you realise" The Straits Times, Apr 14, 2026

⁷Encyclical Letter of His Holiness Leo XIV *Magnifica Humanitas* (May 15, 2026). The Holy See. <https://www.vatican.va/content/leo-xiv/en/encyclicals/documents/20260515-magnifica-humanitas.html>

⁸Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Personal Data Protection Commission Singapore

The guidelines are organised according to the typical stages of the GenAI lifecycle⁹ as presented below:

Stage 1: Collecting and Using Personal Data to train GenAI Models

Applying the “Publicly Available” Exception

Organisations are allowed to collect or use publicly accessible personal data without user consent.¹⁰ However, the tricky part is determining whether personal data that sit behind digital barriers still qualify as publicly available. Organisations must thus carefully assess (i) the purpose and (ii) the complexity of the said digital barrier.

- (i) Purpose e.g. data protected by a paywall that merely serves as a monetisation mechanism is considered publicly available because every buyer will be granted equal access to the data.
- (ii) Complexity e.g. data posted on private social media accounts are not considered publicly available because access to the gated content requires verification of the follower’s identity and the explicit approval by the account owner.

Informing Clients through AI-Specific Notifications

When user data is used for GenAI model development, businesses are required to inform consumers through clear AI-specific notifications.¹¹ While PDPC did not dictate specific presentation forms, the notices should contain thorough information on the functions of the GenAI model and the personal data it digests.

Only when data used is anonymised, i.e. user data has been permanently stripped of all personal identifiers through methods like data masking and generalisation, organisations will not be required to issue AI-specific notifications to their consumers.¹²

Obtaining Client Consent

Client consent is mandatory for the collection, usage or disclosure of personal data. Individuals may withdraw their consent at any time, and the organisation must, in the event of a withdrawal of consent, inform the individual of the likely consequences of the said withdrawal.¹³

However, client consent may come in the form of a deemed consent.¹⁴

⁹PDPC Issues Guidance for Organisations on Responsible Use of Personal Data in Generative AI (Jul 20, 2026). Personal Data Protection Commission. <https://www.pdpc.gov.sg/media-events/pdpc-issues-guidance-for-organisations-on-responsible-use-of-personal-data-in-generative-ai>

¹⁰Section 17(1) of the Personal Data Protection Act 2012

¹¹“Singapore proposes mandatory notification when firms use personal data for AI training” The Straits Times, Jul 13, 2026

¹²“AI-specific notifications mandatory for firms using personal data to train AI models: PDPC” The Straits Times, Jul 21, 2026

¹³Section 16 of the Personal Data Protection Act 2012

¹⁴Sections 15 and 15(A) of the Personal Data Protection Act 2012

Under section 15(1) of the Personal Data Protection Act ("PDPA"), consent is implied if —

- a) the individual, without actually giving consent mentioned in section 14, voluntarily provides the personal data to the organisation for that purpose; and
- b) it is reasonable that the individual would voluntarily provide the data.

Under section 15A(2) of the PDPA, consent can be further implied if —

- a) the organisation satisfies the requirements in subsection (4); and
- b) the individual does not notify the organisation, before the expiry of the period mentioned in subsection (4)(b)(iii), that the individual does not consent to the proposed collection, use or disclosure of the personal data by the organisation.

The requirements in subsection (4) are that the organisation must —

- a) conduct an assessment to determine that the proposed collection, use or disclosure of the personal data is not likely to have an adverse effect on the individual;
- b) take reasonable steps to bring the following information to the attention of the individual:
 - (i) the organisation's intention to collect, use or disclose the personal data;
 - (ii) the purpose for which the personal data will be collected, used or disclosed;
 - (iii) a reasonable period within which, and a reasonable manner by which, the individual may notify the organisation that the individual does not consent to the organisation's proposed collection, use or disclosure of the personal data; and
- c) satisfy any other prescribed requirements.

Stage 2: Processing Personal Data in Deployed GenAI Models

The key stakeholders highlighted below must abide by their specific PDPA obligations outlined by the PDPC.¹⁵

Model Providers

Model Providers are organisations that build the core foundations of the GenAI models for distribution and use e.g. OpenAI and Anthropic. They must strictly abide by the Retention Limitation Obligation¹⁶, which requires these organisations to cease retaining personal data, or

¹⁵Sections 7-9 of the Advisory Guidelines on Use of Personal Data in Generative AI, Personal Data Protection Commission

¹⁶Section 25 of the Personal Data Protection Act 2012

remove the means by which personal data can be associated with particular individuals as soon as it is reasonable to assume that —

- a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and
- b) retention is no longer necessary for legal or business purposes.

Where data is preserved to enhance future models, Model Providers should develop and make accessible data retention policies that include the rationale for retaining data for extended periods of time. These organisations should also regularly review the personal data in their possession to determine if such data is still needed.¹⁷

Furthermore, Model Providers that serve as data intermediaries (i.e. they process personal data on behalf of downstream users) must strictly abide by the Protection Obligation¹⁸, which requires organisations to protect the personal data in its possession or under its control by making reasonable security arrangements to prevent —

- a) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and
- b) the loss of any storage medium or device on which personal data is stored.

System Providers

System Providers are organisations that supply GenAI systems for others to use e.g. Amazon Web Services and Google Cloud Vertex AI. To comply with their Protection Obligation, System Providers are expected to periodically review the need for additional security arrangements as new systems are made available. They are also encouraged to share information about existing safeguards with downstream deployers to uphold greater accountability and facilitate a tighter adherence to these protective protocols.¹⁹

System Deployers

System Deployers are organisations that utilise GenAI systems in their services, whether built in-house or developed by third parties, e.g. DBS Bank (Digibot) and Instagram (Meta AI). These organisations must strictly abide by the Purpose Limitation Obligation²⁰, where they may collect, use or disclose personal data about an individual only for the purposes —

¹⁷Paragraphs 18.5-18.8 of the Advisory Guidelines on Key Concepts in the Personal Data Protection Act, Personal Data Protection Commission Singapore

¹⁸Section 24 of the Personal Data Protection Act 2012

¹⁹Paragraph 8.2-8.3 of the Advisory Guidelines on Use of Personal Data in Generative AI, Personal Data Protection Commission

²⁰Section 18 of the Personal Data Protection Act 2012

- a) that a reasonable person would consider appropriate in the circumstances; and
- b) that the individual has been informed of under section 20 (i.e. through AI-specific notifications), if applicable.

This means that System Deployers should be disciplined in engaging an AI system that only processes the amount of personal data they require.²¹

System Deployers must also comply with their Protection Obligation by implementing security measures to safeguard personal data and conducting regular reviews to evaluate the sufficiency of these protocols. Moreover, they are encouraged to develop clear written policies and document processes in relation to the measures in place to increase the transparency of this security framework.²²

Stage 3: Addressing Consumers' Concerns about Personal Data

Providing Info Cards for GenAI Chatbots

The Chatbot info card serves the critical role of being the consolidated reference point for consumers to access essential information about the chatbot. Hence, it should be designed based on three principles: (i) relevance, (ii) accessibility and (iii) timeliness.²³

(i) Relevance

The info card should disclose a reasonable amount of key information to help users understand how to engage with the chatbot responsibly. Such information includes the capabilities and restrictions of the chatbot, common risks and precautions with regards to using the chatbot, privacy policies, and feedback mechanisms.

(ii) Accessibility

Information should be provided in a meaningful manner. In terms of content, this means that System Deployers should use plain, direct language and provide substantive details to cater to a non-technical audience. In terms of presentation, this means that System Deployers should organise information in a way that promotes readability and facilitates the quick scanning for vital components. The use of visual aids is also greatly recommended. Beyond that, the info card should be readily available to users, such as being displayed as an icon on the chatbot interface or as an identifiable link on the onboarding screen.

²¹Paragraph 13.3 of the Advisory Guidelines on Key Concepts in the PDPA. Personal Data Protection Commission

²²Paragraphs 9.3-9.5 of the Advisory Guidelines on Use of Personal Data in Generative AI, Personal Data Protection Commission

²³Transparency Guidelines for Generative AI Chatbots, Infocomm Media Development Authority

(iii) Timeliness

Information provided in the info card should be the most current to help users keep pace with chatbot developments. To help users verify that they are reading up-to-date information, info cards could include the most recent revision date or the chatbot version to which the info card relates to.

Conclusion

Responsible AI development should never be a choice between innovation and privacy. Rather, privacy should be the cornerstone which every sustainable innovation is built upon.

These new advisory guidelines serve as a crucial reminder that behind every dataset is a person whose information carries dignity. While some of the above-mentioned expectations remain guidelines at the present time, organisations actively involved in the production or utilisation of GenAI models should not procrastinate until they become legally binding orders. Stronger safeguards for personal data should be implemented as soon as possible to give the greatest reassurance to consumers and business partners.

At **INFINITY LEGAL LLC**, we assist and represent clients on all issues relating to personal data protection and privacy.

© Infinity Legal LLC 2026

The content of this article is for general information purposes only and does not constitute legal advice and should not be relied on as such. Specific advice should be sought about your specific circumstances. Infinity Legal LLC does not accept any responsibility for any loss which may arise from reliance on information or materials published in this article. Copyright in this publication is owned by Infinity Legal LLC.

This publication may not be reproduced or transmitted in any or by any means, in whole or in part, without prior written approval.

Infinity Legal LLC thanks and acknowledges Intern Klaire Ho for her contribution to this article.