



July 2026

SINGAPORE'S PDPC ISSUES NEW ADVISORY GUIDANCE ON USE OF PERSONAL DATA IN GENERATIVE AI

Following the conclusion of the Singapore Personal Data Protection Commission's ("PDPC") public consultation on its draft advisory guidelines on the Use of Personal Data in Generative AI (the "**Guidelines**") on 1 July 2026, the PDPC has now published the final version of the Guidelines.

The final Guidelines, which were launched on 20 July 2026 at this year's Singapore Data Festival, set out the PDPC's views on the application of the Singapore Personal Data Protection Act ("**PDPA**") to the use of personal data in training AI models. The Guidelines also outline best practices that organisations at various stages of the AI development lifecycle should adopt to support compliance with the PDPA.

For the purposes of the Guidelines, the AI development lifecycle is broadly divided into three phases – development, deployment, and post-deployment – each of which will be examined in turn in this article.

DEVELOPMENT PHASE: COLLECTING AND USING PERSONAL DATA

1. Publicly Available Exception

In the development phase, the Guidelines place significant focus on the extent to which the "publicly available" exception may be relied upon when processing personal data for the purpose of training AI models.

The "Publicly Available Exception" under the PDPA allows organisations to collect, use or disclose, without consent, personal data about an individual that is publicly available.

Where data is publicly available without any barriers to access, the position is straightforward – organisations may collect and use such data for training AI models without the need to obtain user consent.

However, where access to such data is subject to certain digital barriers, the position becomes more nuanced. Organisations developing Generative AI ("GenAI") models may seek to rely on the "Publicly Available Exception" under the PDPA to web-scrape publicly accessible personal data without obtaining consent. However, where personal data is subject to digital barriers, such as paywalls, registration requirements, or other access restrictions, organisations must carefully assess whether the data can still be considered publicly available under the PDPA.

The Guidelines clarify that the existence of a digital barrier does not, by itself, mean that personal data is no longer publicly available. Rather, organisations will need to undertake a fact-specific assessment in each case. In the GenAI context, relevant factors that organisations should consider in determining whether data may be considered publicly available (and therefore whether it may be used for model training without user consent) include:

- + The purpose of the digital barrier;
- + The effect of the digital barrier;
- + The steps needed (e.g. number, complexity) to access the personal data; and
- + Whether the personal data can be accessed without any restrictions from other online sources.

2. Consent and Notification Obligations

The Guidelines also address the application of the PDPA's "notification obligation" in the context of AI development. Where the "Publicly Available Exception" cannot be relied upon, and user consent is therefore required before personal data may be used for AI model training, the PDPC considers that a general notification which does not specifically identify the intended AI model training use case would be insufficient.

Instead, organisations should provide "AI-Specific Notifications" – clear and explicit notifications that inform individuals that their personal data will be processed for the development and training of AI and/or GenAI models. Such notifications should expressly state the purpose of processing and provide sufficient transparency regarding the intended use of personal data in the AI development process, including details on:

- + Which function(s) of the GenAI model require the use of personal data;
- + That the purpose(s) of collection, use and/or disclosure includes AI and/or GenAI model training and/or fine-tuning;
- + What type(s) of personal data is affected and how the personal data will be used to train or fine-tune the GenAI model; and

- + How individuals may decline or withdraw consent for use of personal data for said purposes (for example, step-by-step instructions or an easily accessible opt-out mechanism).

The Guidelines emphasise that obtaining consent on an earlier occasion does not necessarily permit the subsequent use of personal data for AI or GenAI model development. Where such use represents a material departure from the purposes for which the data was originally collected – such that a reasonable person would not regard the new use as appropriate – organisations are required to obtain fresh consent.

The Guidelines also reiterate that organisations must not make an individual's consent to the collection, use or disclosure of personal data for training or fine-tuning GenAI models a condition of providing a product or service, except to the extent that such processing is reasonably necessary for the provision of that product or service.

DEPLOYMENT PHASE: DATA PROTECTION RESPONSIBILITIES OF STAKEHOLDERS

In the deployment phase of an AI model, the Guidelines focus on the different responsibilities of different stakeholder organisations, including:

1. **Model Providers** that process personal data to develop or deploy GenAI models are considered organisations under the PDPA and must comply with its obligations and pay particular attention to data retention issues. When processing data on behalf of downstream stakeholders, they should also document and share information on model-level safeguards.
2. **System Providers** that use personal data to develop GenAI systems are similarly subject to PDPA obligations. Where they process data on behalf of downstream users, they should ensure appropriate security safeguards are in place and share relevant information on system-level protections with downstream deployers.
3. **System Deployers** bear primary responsibility for PDPA compliance, including defining clear



purposes for personal data processing, safeguarding data flowing through their systems, and regularly reviewing safeguards – especially for agentic AI systems.

The Guidelines note that a single organisation may perform more than one of these roles across different contexts and, if so, will need to consider its obligations in each role.

POST DEPLOYMENT PHASE: HANDLING DATA SUBJECT REQUESTS

The Guidelines acknowledge the practical challenges associated with complying with the PDPA's access and correction obligations in the context of Generative AI, particularly given the vast volumes of data used to train models and the technical limitations involved in identifying, retrieving or amending personal data within those models.

Nevertheless, the Guidelines make clear that these challenges do not relieve organisations of their obligations under the PDPA.

Organisations are expected to take reasonable steps to facilitate access and correction requests and, where appropriate, adopt best practices to support compliance. These include:

- + Implementing robust upstream data governance measures, such as verifying the accuracy of personal data at the point of collection, applying data cleansing processes and maintaining data provenance records;
- + Assessing access and correction requests on a case-by-case basis and complying with such requests where reasonable;
- + Removing personal data, including inaccurate personal data, from training datasets where feasible;
- + Deploying output filters and other safeguards to minimise the likelihood of inaccurate personal data being generated as outputs; and
- + Progressively adopting appropriate technical measures to enable the removal of inaccurate personal data from Generative AI models and systems.

CONCLUSION

The Guidelines represent one of the first efforts globally by a data protection regulator to apply and provide practical guidance on the application of data protection principles and legislation to the use of personal data in AI model training – an emerging issue that regulators in other jurisdictions, including the UK and the EU, continue to grapple with.

CONTACT US



SHEETAL SANDHU

Partner at Virtus Law

+65 6661 6523
sheetal.sandhu
@stephensonharwood.com



SHU WEI LEE

Associate at Virtus Law

+65 6661 6893
shuwei.lee
@stephensonharwood.com



DOUG HENDERSON

Associate

+44 20 7809 2871
doug.henderson
@stephensonharwood.com

The Singapore law aspects of this article were written by members of Virtus Law (a member of the Stephenson Harwood (Singapore) Alliance).