WONG PARTNERSHIP

Use of Personal Data in GenAI

PDPC Issues Advisory Guidelines on Use of Personal Data in GenAI

On 20 July 2026, the Personal Data Protection Commission (**PDPC**), with support from the Infocomm Media Development Authority (**IMDA**), issued the Advisory Guidelines on Use of Personal Data in Generative AI (**Guidelines**), guidance applicable to organisations that collect and use personal data in Generative AI (**GenAI**) Models and Systems. The Guidelines incorporate feedback from PDPC's public consultation on its Proposed Advisory Guidelines on use of Personal Data in Generative AI, which closed on 1 July 2026 and which we covered in an earlier update.

The Guidelines clarify how the Personal Data Protection Act 2012 (**PDPA**) applies as more organisations incorporate GenAI into their work processes, including: (a) how personal data can be collected and used to develop GenAI models; (b) the allocation of data protection responsibilities across the GenAI lifecycle; and (c) how individuals' requests concerning the processing of their personal data for GenAI should be handled.

They build on and should be read in conjunction with the PDPC's Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems and Advisory Guidelines on Key Concepts in the PDPA. They should also be read in conjunction with any other relevant guidelines that the PDPC issues from time to time.

The Guidelines are advisory in nature and not legally binding. They neither modify nor supplement the legal effect and interpretation of the PDPA and its subsidiary legislation, which prevail over the Guidelines in the event of any inconsistency. The Guidelines should not be construed to limit or restrict the PDPC's administration and enforcement of the PDPA.

Key Takeaways

- The PDPC, with support from IMDA, has issued Advisory Guidelines clarifying how the PDPA applies to the use of personal data in GenAI Models and Systems.
- Organisations may rely on the Publicly Available Exception in lieu of seeking consent to web-scrape publicly available personal data to develop a GenAI Model, subject to the test of a reasonable person considering the use of personal data to develop the GenAI Model appropriate in the circumstances. However, where personal data forms part of online data behind a digital barrier, organisations must assess that the personal data is publicly available before they can rely on the Publicly Available Exception.
- General Notifications, which cite the use of personal data for "new product development" without specifying AI or GenAI Model development, are insufficient to obtain consent to use personal data provided by an individual or created during or following the individual's use of the organisation's products or services (**User Data**) for large-scale GenAI Model training and/or fine-tuning.

Key Takeaways

- Organisations must provide an explicit statement that the purpose of processing includes AI and/or GenAI Model development (**AI-Specific Notifications**) to obtain consent for the use of User Data.
- Model Providers, System Providers, and System Deployers bear distinct PDPA responsibilities across the GenAI lifecycle, with System Deployers bearing primary responsibility for ensuring the GenAI Systems they have chosen to use can meet their obligations under the PDPA.
- Individuals can request access to and correction of their personal data even after it has been used in GenAI development.

The key recommendations for each lifecycle stage (Development, Deployment, and Post-Deployment) are set out below.

Development: Collecting and Using Personal Data to Develop GenAI Models

Organisations developing GenAI models may rely on the Publicly Available Exception under the PDPA to web-scrape publicly accessible personal data in lieu of consent. However, where personal data sits behind digital barriers, such as paywalls, registration requirements or authentication mechanisms, organisations must assess that the data is publicly available before they can rely on the Publicly Available Exception.

In the Generative AI context, relevant factors that organisations should consider in their assessments include:

(a) The purpose of the digital barrier (e.g., to enable data monetisation);

(b) The effect of the digital barrier (e.g., whether the online data remains accessible to the public at large or only a specific group of persons);

(c) The steps needed (e.g., number, complexity) to access the personal data; and

(d) Whether the personal data can be accessed without any restrictions from other online sources.

Example 1

A technology company web-scraping to train a GenAI model identifies a dataset with personal data only available on a database for members of specified professional bodies, where sign-up requires membership or professional registration details. Because the registration requirements confine data access to a specific group and the data is not otherwise accessible, the company concludes that the personal data is likely not publicly available.

Where User Data is used for GenAI model development, and exceptions to consent do not apply, organisations must obtain meaningful consent by providing AI-Specific Notifications. These notifications should, to the extent practicable, provide:

(a) The function(s) of the GenAI Model that require(s) the use of personal data;

(b) A clear description of the type(s) of personal data that will be used to develop the GenAI Model;

(c) How personal data will be used to train and/or fine-tune the GenAI Model; and

(d) How individuals can decline or withdraw consent to the use of personal data for AI training.

Example 2

An apparel company that rebrands as a GenAI model developer and intends to use its User Data (e.g., customer names, transaction histories, and behavioural data) for training to gain a commercial advantage determines that using such personal data is so significant a departure from past commercial activities that a reasonable person would not consider the use to be appropriate. It therefore cannot rely on the business improvement exception. The appropriate course is to obtain fresh consent.

Notwithstanding the above, organisations are encouraged to anonymise their datasets as much as possible and/or practice data minimisation when developing GenAI Models, to minimise unnecessary risks. Where personal data is necessary for GenAI development, organisations should implement appropriate physical, technical, process and legal controls for data protection.

Deployment: Processing Personal Data in Deployed GenAI Models and Systems

Three key stakeholders bear distinct PDPA responsibilities:

(a) **Model Providers**: must comply with all PDPA obligations when they process data to develop and deploy GenAI Models, and pay particular attention to their "Retention Limitation Obligation". Section 25 of the PDPA requires an organisation to cease to retain its documents containing personal data, or remove the means by which personal data can be associated with particular individuals, when the purpose for collecting the data is no longer being served and retention is no longer necessary for legal or business purposes. When processing personal data on behalf of downstream stakeholders, Model Providers must protect personal data in their possession or under their control by making reasonable security arrangements (Protection Obligation). It is good practice to document and make available the measures they have taken to safeguard personal data from downstream sources.

(b) **System Providers**: where System Providers process personal data as part of their own datasets to develop systems, they are organisations. Where they process personal data on behalf of downstream deployers, they are data intermediaries and should periodically review the need for additional security arrangements as they develop and make available new types of systems. It is good practice to share information on the GenAI system-level security

arrangements implemented with downstream deployers. Examples of relevant information include: data security and protection measures around the development environment; testing and performance metrics; and incident response and data breach procedures.

For more transparency best practices, System Providers may wish to refer to IMDA's Transparency Guidelines for Generative AI Chatbots.

(c) **System Deployers**: bear primary responsibility for ensuring that the GenAI Systems they have chosen to use can meet their obligations under the PDPA. When procuring systems, they must therefore ensure that they have sufficient information on upstream safeguards to conduct a holistic assessment. They must also ensure that personal data processed by their chosen system is for relevant purposes and to the extent that a reasonable person would consider appropriate in the circumstances.

They must also safeguard new categories of data sources collected through their systems, and track and designate responsibilities over new data sources and implement corresponding safeguards. System Deployers are further encouraged to develop clear written policies and document processes in relation to the safeguards undertaken. As AI risks continue to evolve, System Deployers should regularly review the sufficiency of their safeguards, especially where their GenAI Systems have agentic functionalities. While the definition of AI agents remains unsettled, common features include independent planning and action taking across multiple steps, often involving access to external tools and systems, to achieve user-defined objectives. These enhanced capabilities can exacerbate data protection risks and complicate responsibility allocation. System Deployers should carefully consider and be transparent about the privacy-utility trade-offs when scoping their agentic use cases. For further guidance on managing agentic risks, organisations may refer to IMDA's Model AI Governance Framework for Agentic AI.

Post-Deployment: Addressing Individuals' Requests About Personal Data

Individuals can request to access and correct their personal data even after it has been used in GenAI development. The PDPC recognises the challenges in facilitating GenAI-related access and correction requests. These arise, for instance, from the massive amounts of data used to develop GenAI Models and/or Systems, which can make it difficult to identify, verify and correct personal data of specific individuals; and the nature of GenAI Models and/or Systems (e.g., the fact that training data is not stored in a traditional repository but as embeddings, and User Data is temporarily held in context windows).

Where reasonable and appropriate in the circumstances, organisations are expected to adopt best practices to support compliance with their Access and Correction Obligations:

(a) Adopt upstream data handling measures such as: (i) verifying data accuracy at the point of collection; (ii) implementing data cleaning techniques like de-duplication and outlier detection; and (iii) maintaining data provenance records to document the lineage of training data;

(b) Review access and correction requests on a case-by-case basis and accede where reasonable, as well as ensure that personal data, including inaccurate data, is removed from training datasets before they undertake future AI training runs; and

(c) Track the maturity of, and progressively adopt, appropriate technical measures to remove inaccurate personal data from models and systems. In the interim, organisations may consider output filters and other safeguards to minimise the likelihood of models or systems producing inaccurate data as outputs.

If you would like information and/or assistance on the above or any other area of law, you may wish to contact the Partner at WongPartnership whom you normally work with or any of the following Partners:

LAM Chung Nian
Head – Intellectual Property, Technology & Data

Kylie PEH
Partner – Intellectual Property, Technology & Data

Connect with WongPartnership.

WPG MEMBERS AND OFFICES

- contactus@wongpartnership.com

SINGAPORE

-
WongPartnership LLP
12 Marina Boulevard Level 28
Marina Bay Financial Centre Tower 3
Singapore 018982
t +65 6416 8000
f +65 6532 5711/5722

CHINA

-
WongPartnership LLP
Shanghai Representative Office
Unit 1015 Link Square 1
222 Hubin Road
Shanghai 200021, PRC
t +86 21 6340 3131
f +86 21 6340 3315

INDONESIA

-
Makes & Partners Law Firm
Menara Batavia, 7th Floor
Jl. KH. Mas Mansyur Kav. 126
Jakarta 10220, Indonesia
t +62 21 574 7181
f +62 21 574 7180
w makeslaw.com

MALAYSIA

-
Cheang & Ariff
Advocates & Solicitors
Loke Mansion
273A, Jalan Medan Tuanku
50300 Kuala Lumpur
t +60 3 2691 0803
f +60 3 2693 4475
w cheangariff.com
-
Foong & Partners
Advocates & Solicitors
13-1, Menara 1MK, Kompleks 1 Mont' Kiara
No 1 Jalan Kiara, Mont' Kiara
50480 Kuala Lumpur, Malaysia
t +60 3 6419 0822
f +60 3 6419 0823
w foongpartners.com

MIDDLE EAST

-
Al Aidarous Advocates and Legal Consultants
Abdullah Al Mulla Building, Mezzanine Suite 02
39 Hameem Street (side street of Al Murroor Street)
Al Nahyan Camp Area
P.O. Box No. 71284
Abu Dhabi, UAE
t +971 2 6439 222
f +971 2 6349 229
w aidarous.com
-
Al Aidarous Advocates and Legal Consultants
Oberoi Centre, 13th Floor, Marasi Drive, Business Bay
P.O. Box No. 33299
Dubai, UAE
t +971 4 2828 000
f +971 4 2828 011

PHILIPPINES

-
Gruba Law
27/F 88 Corporate Center
141 Valero St., Salcedo Village
Makati City 1227, Philippines
t +63 2 889 6060
f +63 2 889 6066
w grubalaw.com