

ANNEXURE D

Suggested Wording for the Framework Paragraphs Our Recommendations Touch

To: Submission of Edwin Lee & Partners on Public Consultation Paper No. 1/2026: Artificial Intelligence (AI) and Personal Data Protection Framework

How to read this Annexure

The Core Submission says what we think should change and why. This Annexure offers wording for the paragraphs concerned, so that the drafting team has something concrete to work from if it finds any of our recommendations useful. The wording is a starting point only. JPDP's own drafting conventions govern, the Bahasa Malaysia text is the authoritative one, and we have drafted in English because that is the language of our submission.

Entries are in Framework order. For each, we give the current text where we propose to change it, the suggested text, and the recommendation it comes from. New paragraphs are numbered provisionally.

Part A: Introduction

New paragraph 2.2 (status and effect) [Recommendation 1]

Suggested text:

2.2 This Framework sets out the Commissioner's view of what Act 709, and in particular the Personal Data Protection Principles, require where personal data is processed through AI systems. In assessing whether a data controller has complied with Act 709, the Commissioner will take into account whether the data controller has followed this Framework. A data controller that departs from any provision of this Framework should be able to show, in writing, why the departure was appropriate having regard to the nature, scope, context and purpose of the processing and the risks to data subjects.

New paragraph 2.3 (relationship with other instruments) [Recommendation 1]

2.3 This Framework is to be read together with the guidelines, circulars and standards issued by the Commissioner, including the Guideline on Automated Decision-Making and Profiling, the Data Protection Impact Assessment Guideline, the Data Protection by Design Guideline, the Guidelines on the Appointment of Data Protection Officer, the Guidelines on Cross-Border Personal Data Transfer, Circular No. 1/2025 and Circular No. 2/2025, and the Personal Data Protection Standard 2015. Where this Framework and another instrument address the same matter, the table at Appendix [X] identifies the instrument that applies. Nothing in this Framework relaxes any requirement in those instruments.

New paragraph 2.4 (relationship with the AI Governance Bill) [Recommendation 10]

2.4 This Framework governs the processing of personal data through AI systems. A Data Protection Impact Assessment conducted in accordance with this Framework is intended to satisfy, in respect of personal data, any corresponding assessment required under any written law governing AI systems, and the Commissioner will review this Framework for alignment with such law when it is enacted.

Part B: Definitions and Scope

Paragraph 4.1 [Recommendation 2(a)]

Current text: "AI systems may use software, algorithms, machine learning models, predefined rules or other computational methods, individually or in combination, in performing their functions."

Suggested text:

4.1 AI systems may use software, algorithms, machine learning models or other computational methods, individually or in combination, in performing their functions. A system that operates solely on fixed, pre-defined rules determined by natural persons, and that does not learn from data or infer from patterns, is not an AI system for the purposes of this Framework, even where its outputs take the form of predictions, recommendations or decisions.

New paragraph 4.9 (application by level) [Recommendation 2(b)]

4.9 This Framework applies in full to an AI system that makes, or materially supports, decisions that produce legal effects or similarly significant effects on a data subject. For any other AI system, Parts C, F and H apply, together with a record under Part J that is proportionate to the processing, and the remaining Parts are to be read as good practice.

New definition in paragraph 3.2 [Recommendation 11(a)]

"biometric data" has the meaning given in section 4 of Act 709, and includes personal data resulting from technical processing of a person's face, voice, gait, keystroke pattern or facial expression [whether or not the data is used to identify the person].

The bracketed words reflect the reading of the section 4 definition that we think is correct (Core paragraph 12.3). They should be included only if the Commissioner adopts that reading.

New paragraph 4.10 (anonymised data) [Recommendation 2(d)]

4.10 Personal data that has been anonymised in accordance with this Part is no longer personal data for the purposes of Act 709. A data controller that discloses de-identified data to another person should require that person, by contract, not to attempt to re-identify any data subject.

Part C: Legal Basis for Processing

Paragraph 6.3 [Recommendations 4(a) and 4(c)]

Current text (in part): "... remain consistent with the purpose for which the personal data was collected or made available."

Suggested text:

6.3 Where personal data is obtained from third-party sources, publicly available sources or external datasets for AI-related processing, the data controller remains responsible for ensuring that the collection and subsequent processing comply with Act 709. The fact that personal data is publicly available does not remove the requirements of sections 6 and 7 of Act 709 and does not amount to the data subject's consent. The processing must be for the purpose for which the personal data was collected or made available, or a purpose directly related to it; otherwise notice under section 7 and, where no ground under subsection 6(2) applies, consent under section 6 are required. A data controller should also note section 130 of Act 709, which prohibits the knowing or reckless collection of personal data held by another data user without that data user's consent.

Paragraph 7.4 (first two sentences) [Recommendation 4(a)]

Current text: "Where the data controller intends to process personal data through AI systems for a purpose not previously specified in the written notice, the data controller shall provide a new or revised written notice ... Where consent is required under Act 709, fresh consent shall also be obtained."

Suggested text:

7.4 Where the data controller intends to process personal data through AI systems for a purpose other than the purpose specified in the written notice, or a purpose directly related to it, the data controller shall provide a new or revised written notice to the data subject before commencing such processing, in accordance with paragraph 7(2)(c)(i) of Act 709. Where no ground under subsection 6(2) of Act 709 applies, consent for the new purpose shall also be obtained.

Paragraph 8.3(d) [Recommendation 4(a)]

Current text: "fresh consent is obtained where the intended purpose of processing materially differs from the purpose originally consented to by the data subject, unless the processing is otherwise permitted under Act 709."

Suggested text:

(d) fresh consent is obtained where the intended purpose of processing is not the purpose consented to by the data subject or a purpose directly related to it, unless the processing is otherwise permitted under Act 709.

New paragraph 9.5 (biometric data created by AI systems) [Recommendation 11(b)]

9.5 An AI system may create biometric data from personal data that is not itself biometric, for example by processing images, audio, video or behavioural signals to produce data relating to a person's physical, physiological or behavioural characteristics. Such data is sensitive personal data. Before an AI system that creates biometric data is deployed, the data controller shall obtain the data subject's explicit consent or satisfy another condition under section 40 of Act 709, shall give the data subject a specific notice of the processing, and, where the purpose can reasonably be achieved without biometric processing, shall provide an alternative for data subjects who do not consent.

Paragraph 10.4 (addition at the end) [Recommendation 4(d)]

The exemption for processing for research or statistical purposes under paragraph 45(2)(c) of Act 709 applies only where the personal data is not processed for any other purpose and the results are not made available in a form that identifies any data subject. It will not ordinarily apply to the development of an AI system intended for commercial deployment, or to any model from which personal data can be retrieved or reproduced.

Part D: Development and Testing

Paragraph 12.4 [Recommendation 4(b)]

Current text: "... the data controller shall consider the use of anonymised or pseudonymised data ..."

Suggested text:

12.4 Where the intended purpose of development, training, testing or validation can reasonably be achieved without directly identifying the data subject, the data controller shall use anonymised or pseudonymised data, having regard to the safeguards set out in Part H of this Framework. The process of anonymising or pseudonymising personal data is itself processing of personal data and requires a basis under Act 709 until the data ceases to be personal data.

New paragraph 12.5 (assessing whether training is directly related to the original purpose) [Recommendation 4(b)]

12.5 In assessing whether the use of personal data to develop, train, fine-tune or improve an AI system is directly related to the purpose for which the personal data was collected, the data controller shall have regard to: (a) the link between that use and the purpose specified in the written notice; (b) what the data subject was told and could reasonably expect; (c) whether sensitive personal data is involved; (d) the likely effect on the data subject, including the risk that the AI system reproduces the personal data in its outputs; and (e) the safeguards applied, including anonymisation or pseudonymisation before training. Example: retraining a fraud-detection model on the data controller's own transaction records, for the fraud-prevention purpose specified at collection, will ordinarily be directly related to that purpose. Training a general customer-service assistant on correspondence collected to handle individual customers' matters, where the assistant will serve other customers or be licensed to other businesses, will ordinarily be a new purpose requiring notice and, where no ground under subsection 6(2) applies, consent.

Paragraph 14 (new sub-paragraph) [Recommendation 5]

14.6 Before testing begins, the data controller shall document the acceptance criteria against which the AI system will be assessed and the version of the AI system under test, and shall record the results of testing against those criteria.

Part F: Procurement and Use of External AI Systems

Paragraph 21.2 (addition) [Recommendations 6(a) and 6(b)]

An AI service provider that processes personal data only to provide the service to the data controller, in accordance with the data controller's instructions, and that does not use the personal data for its own purposes, is ordinarily a data processor. An AI service provider whose terms permit it to use personal data supplied through the service to train, improve or evaluate its own AI models, or for any other purpose of its own, is to that extent a third party under Act 709, and the data controller requires a basis under sections 6 and 8 and, for sensitive personal data, section 40, before any personal data is processed through the service for that purpose. An AI service provider may be a data processor for some processing and a third party for other processing under the same terms. In making this determination the data controller may rely on the provider's data processing terms, its published commitments on retention and training, and the documentation referred to in paragraph 21.4.

Paragraph 22.2 (addition) [Recommendation 6(e)]

A Transfer Impact Assessment shall be conducted for any external AI system that processes personal data outside Malaysia. In addition to the matters set out in the Guidelines on Cross-Border Personal Data Transfer, the assessment shall consider: (a) where the personal data is stored and processed, including by any sub-processor; (b) the law of the destination governing access by public authorities to personal data held by service providers; and (c) the independent oversight and avenues of redress available to a data subject in Malaysia in respect of such access.

New paragraph 22.5 (models deployed by the data controller) [Recommendation 6(f)]

22.5 Where a data controller deploys an AI model on infrastructure under its own control, whether its own systems or a cloud environment located in Malaysia, such that no personal data is transmitted to the developer of the model or to any person outside Malaysia, the processing does not involve a transfer under section 129 of Act 709 and paragraph 22 does not apply. Such deployment may constitute a data protection by design measure under Part D. The data controller remains responsible for the security, testing, monitoring and maintenance of the AI system under Parts D, E and H.

Part G: Rights of Data Subjects

New paragraph 29.4 (application of rights to AI systems) [Recommendation 7]

29.4 For the purposes of this Part: (a) inferences, scores and profiles generated by an AI system about an identifiable individual are personal data, and are within the right of access where they can reasonably be identified and retrieved; (b) the weights and parameters of an AI model are not personal data; (c) prompts, inputs and outputs retained by the data controller that contain personal data are subject to the Retention Principle and the right of access; (d) where an AI system causes or contributes to an inaccuracy, the data controller shall correct the personal data held and prevent further reliance on the inaccurate output, but is not required to retrain the AI system; (e) on withdrawal of consent, the data controller shall cease processing the personal data through the AI system and delete it from any store from which it can be retrieved, but is not required to retrain an AI model in which the personal data can no longer be identified; and (f) [personal data generated by an AI system about the data subject is not within the right to data portability under section 43A of Act 709].

The bracketed limb (f) reflects our reading of section 43A (Core paragraph 8.3) and should be included only if the Commissioner adopts it.

New paragraph 29.5 [Recommendation 7]

29.5 A data subject may exercise the right under section 42 of Act 709 to require a data controller to cease, or not to begin, processing through an AI system that is causing or is likely to cause unwarranted substantial damage or distress to him or to another person, subject to subsection 42(2). Act 709 does not otherwise confer a right to object to automated decision-making or profiling or a right to require human review of a decision, and nothing in this Framework creates such a right.

Part H: Fairness, Security and Breach

Paragraph 31.1 (addition at the start) [Recommendation 8(a)]

31.1 In accordance with the General Principle and the Data Integrity Principle of Act 709, AI systems that process personal data shall be designed, tested, used and monitored ...

Paragraph 33.5 [Recommendation 8(d)]

Current text: "... to enable timely communication of information necessary for the data controller to comply with section 12B of Act 709."

Suggested text:

33.5 Where a personal data breach involves a data processor or AI service provider, the data controller shall ensure that appropriate arrangements are in place requiring the data processor or AI service provider to notify the data controller of the breach without undue delay and in any event within [24] hours of becoming aware of it, and to provide the information necessary for the data controller to comply with section 12B of Act 709 and Circular No. 1/2025, including the AI system or model and version involved.

Part I: Governance and Risk Management

Paragraph 35.4 [Recommendation 3(b)]

Current text: "Where a Data Protection Officer is appointed or required under Act 709, the Data Protection Officer shall be appropriately involved in the oversight of personal data processing through AI systems, having regard to the nature and risks of the processing."

Suggested text:

35.4 Where a Data Protection Officer is appointed or required under Act 709, the Data Protection Officer shall be involved in the oversight of personal data processing through AI systems. Where an AI system makes or materially supports decisions that produce legal or similarly significant effects on data subjects, the Data Protection Officer shall be involved from the design stage, consistently with the Guideline on Automated Decision-Making and Profiling. Whether a Data Protection Officer must be appointed is determined by Circular No. 2/2025 and the Guidelines on the Appointment of Data Protection Officer, and not by the use of an AI system as such.

Paragraph 37.2(a) [Recommendation 11(c)]

(a) the type, volume, nature and sensitivity of personal data processed, including any sensitive personal data, such as biometric data, that the AI system may create from other personal data;

Paragraph 37.3 [Recommendations 3(a) and 11(d)]

Current text: "Where appropriate, the risk assessment shall include, or be complemented by, a Data Protection Impact Assessment (DPIA) ..."

Suggested text:

37.3 The risk assessment shall include, or be complemented by, a Data Protection Impact Assessment (DPIA) conducted in accordance with the Data Protection Impact Assessment Guideline, where the AI system makes or materially supports decisions that produce legal or similarly significant effects on data subjects, where the AI system processes or creates biometric data, or where a DPIA is otherwise required under that Guideline or the Guideline on Automated Decision-Making and Profiling. In other cases the data controller shall consider whether a DPIA is appropriate. The DPIA shall be completed before the relevant processing begins.

Part J: Documentation and Audit

Paragraph 42.3(c) [Recommendation 3(c)]

Current text: "risk assessments and Data Protection Impact Assessments, where conducted;"

Suggested text:

(c) risk assessments and Data Protection Impact Assessments required under paragraph 37 or the applicable guidelines, and any other assessments conducted;

Paragraph 40.4 (addition) [Recommendation 9]

(i) the identity and version of the AI system or model concerned, the date of the record and the person responsible for it.

This document is prepared by Edwin Lee & Partners. It is submitted in response to a public consultation and does not constitute legal advice to any person. The wording above is offered to assist the drafting team and is not a statement of the law. Specific advice should be sought for particular circumstances.