

ANNEXURE A

Response Matrix: ELP Submission Keyed to the Seven Consultation Questions

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

Reference: Consultation Paper, Part 3, questions 4.1.1 to 4.1.7

How to read this Annexure

The Consultation Paper asks seven questions. This matrix gives our answer to each in a few paragraphs, points to where the reasoning is developed in the Core Submission, and lists the recommendations that respond to it. The answers we have given in the official Google Form are the same as the answers here, in shorter form.

Paragraph numbers in the second column refer to the Framework. Paragraph numbers in the third column refer to the Core Submission.

The matrix

Question	Our answer	Core paras	Recs
1. Is the proposed Framework adequate to support compliance with Act 709 in the development and deployment of AI systems involving personal data? If not, which aspects need improvement or clarification?	Largely yes. The Framework stays close to Act 709, correctly says that AI creates no separate legal basis (para 5.1), handles offshore processing through section 129 (para 22), and contains a fairness obligation built from Malaysian materials (para 31). We support it. Four aspects need clarification. First, its legal effect: it is a guideline under subsection 48(g) written in mandatory terms, and it does not say what follows if a controller departs from it. A short status-and-effect clause on a comply-or-explain basis would settle this. Second, its relationship with the ADMP Guideline, which it never mentions and now contradicts on whether a DPIA is required, when the DPO must be involved, and whether AI may be the sole basis of a decision. Third, the legal basis for training or fine-tuning on personal data the controller already holds: the Framework states the reuse test three different ways (paras 6.3, 7.4, 8.3(d)), none of them the Act's own "directly related" test, and does not say how the test applies to training. Fourth, data subject rights in AI systems (Part G), where six practical questions can be answered now, where the Framework should mention the section 42 notice as the data subject's existing remedy against harmful AI processing, and where it should say that Act 709 gives no further right to object to profiling or to require human review.	2.1 to 2.5; 4.1 to 4.5; 5.1 to 5.8; 8.1 to 8.4	1, 3, 4, 7

Question	Our answer	Core paras	Recs
2. Apart from the proposed scope and definitions, are there additional concepts, circumstances, limitations or exemptions that should be considered? Please give proposals with justification and use cases.	Four. (a) An exclusion for systems that run only on fixed, pre-defined rules without learning from data or inferring from patterns. Paragraph 4.1 currently includes "pre-defined rules" in the definition, which would bring a deterministic compliance questionnaire (our own, for example) within the Framework. Use case: a rules-based DPIA tool, a scoring spreadsheet, a fixed decision tree. (b) A two-level reference point for "proportionate", which the Framework uses at least seven times without saying proportionate to what. AI systems that make or materially support decisions with legal or similarly significant effects attract the Framework in full; others attract Parts C, F, H and a short record. The trigger is the one the ADMP Guideline already uses. Use case: a CRM with an AI recommendation feature versus an AI credit-scoring model. (c) A table mapping the "AI Service Provider" onto the data processor and third party under Act 709, since the Framework's term cuts across the Act's categories and a processor is subject to the Security Principle only. The same table should distinguish a hosted AI service from a model run on the controller's own infrastructure, which involves no transfer under section 129. (d) A definition of biometric data by reference to section 4, as amended in 2024. The Framework never mentions biometric data, although AI systems create it from voice, images and behaviour, and it is sensitive personal data requiring explicit consent under section 40. Use case: a call-centre voice-analytics add-on; a retail camera that reads mood.	3.1 to 3.6; 7.9; 12.1 to 12.5	2, 6(f), 11

Question	Our answer	Core paras	Recs
3. Is the proposed approach adequate to ensure personal data is processed lawfully, fairly, transparently, securely and responsibly across the AI lifecycle? Please give specific suggestions on principles, controls or best practices.	The approach is sound. Our specific suggestions, in lifecycle order: Legal basis (Part C): restate paras 6.3, 7.4 and 8.3(d) using the Act's "directly related" test; set out the factors for applying it to training, with one worked example; say that public availability does not displace sections 6 and 7 and that collection from another data user's sources may engage section 130; say how far the research exemption reaches; and say that anonymising data is itself processing. Development and testing (Parts D, E): give indicative triggers for "material change" in para 18.1, and require acceptance criteria and the version under test to be recorded before testing starts (para 14). Procurement (Part F): describe the common provider set-ups under para 21.2; state that where a service's terms allow the provider to train on inputs, the provider is a third party and the controller needs a basis under sections 6, 8 and 40 before any personal data goes in, with three compliant routes at three cost levels; say what a controller may rely on when training-data information cannot be obtained (para 20.2(c)); connect para 16.4 on unauthorised use to acceptable-use policies and controls; make the Transfer Impact Assessment the norm for external AI services and have it cover storage location, the destination's law on public-authority access, and redress; and recognise local deployment of a model as a data-protection-by-design measure. Rights (Part G): six clarifications on inferences, model weights, logs, correction, withdrawal and whether AI-generated data falls within portability under section 43A. Fairness, security, breach (Part H): anchor para 31 to the General and Data Integrity Principles; cross-refer the Standard 2015 and the Cyber Security Act 2024; add four AI-specific fields to the breach form; state the notification window expected from processors. Oversight: define human oversight by capability (understanding, information, authority) and state the ADMP Guideline's no-sole-factor rule for significant decisions.	4.4 to 4.5; 5.2 to 5.5; 6.1 to 6.2; 7.3 to 7.11; 8.3; 9.3 to 9.5	3, 4, 5, 6, 7, 8

Question	Our answer	Core paras	Recs
4. Are the proposed governance, safeguards, risk management and accountability measures clear, practical and proportionate to risk levels, roles and organisational capability? What improvements are needed?	Clear and well-intentioned, but not yet proportionate in a way a small controller can apply, for three reasons. First, "proportionate" has no reference point; see our answer to question 2(b). Second, the DPIA position is unclear. Para 37.3 makes it "where appropriate", para 42.3(c) treats it as something kept "where conducted", and the ADMP Guideline makes it mandatory whenever automated decision-making is present. The three should say the same thing: required where the system makes or materially supports decisions with significant effects, otherwise discretionary. The Framework should also keep the duty to assess separate from the duty to appoint a DPO, which is governed by Circular No. 2/2025 and not by the use of AI as such, and should recognise that the DPIA Guideline lets a suitable person other than the DPO lead an assessment. Third, records. Paras 39.3, 40.4 and 42.3 list overlapping records three times. One AI Processing Record, published as a template, scaled to the reference point, able to sit alongside the records the controller already keeps under section 44 and the Commissioner's guidelines, and specified so that its source-of-data entry also serves as the training-data source record under any future text and data mining exception, would replace all three and make JPDP's supervision easier. Each record should identify the AI system and version concerned. A worked example of how the current draft lands on a 25-staff retailer with no in-house lawyer is at Core paragraph 5.8.	3.4; 4.3 to 4.4; 10.1 to 10.5	2(b), 3, 9

Question	Our answer	Core paras	Recs
5. What constraints or challenges might organisations face if the requirements in this Framework are enforced under Act 709? Please suggest mitigation measures.	The first constraint is not knowing whether the requirements are enforced at all, and on what basis. Larger controllers will treat every "shall" as binding; smaller ones will treat a guideline as optional. Mitigation: the status-and-effect clause in Recommendation 1. The second is requirements that cannot be met as written. Para 20.2(c) asks for training-data information general-purpose model providers do not disclose; para 22.2's Transfer Impact Assessment, done separately by every SME for the same handful of services, is wasted effort; para 33.5 asks controllers to get breach information from providers "in time" without saying what that means. Mitigation: state what a controller may rely on instead of unobtainable information; publish a TIA template or assessments of common destinations; state the notification window expected of processors. The third is cost, and here we would be candid. An enterprise AI subscription is beyond many Malaysian businesses. The answer is not to lower the legal standard, which the Act sets, but to show the free and cheap routes to compliance: keep personal data out of consumer tools altogether; use a working training opt-out, verified and recorded, for non-sensitive data; or run a model locally. Mitigation: the three routes in Recommendation 6(b) and the local-deployment point in Recommendation 6(f). The fourth is the record-keeping burden described under question 4. Mitigation: Recommendation 9.	2.3; 7.4 to 7.9; 9.5; 10.1 to 10.4	1, 6, 8(d), 9

Question	Our answer	Core paras	Recs
6. What preparations do stakeholders need before the requirements are implemented or enforced? What regulatory support (supplementary guidelines, transition periods, sandboxes) is needed?	Controllers need to be able to find out, without paying for advice, which of the Framework's requirements apply to them and what a compliant arrangement looks like. The support that would do most, in order: (a) Templates published with the Framework: the AI Processing Record; a short Transfer Impact Assessment template for external AI services; a one-page note on role determination under para 21.2; a checklist of what to look for in a provider's standard terms; and non-mandatory model clauses for para 21.3 for the cases where the controller can negotiate. We offer starting points for the last two at Annexure C. The Framework should also say that, for a service on standard terms, the provider's published terms and data processing addendum, the controller's configuration of the service and its record of both can together constitute the arrangements paragraph 21.3 requires. (b) A dedicated enquiry channel at JPDP for AI-related questions. (c) A transition period of twelve months from publication, the first six months clearly guidance-only. Our experience with the DPO requirements is that smaller controllers learned the rules applied to them only after the deadline. (d) Any sandbox designed together with the National AI Office and using existing national sandbox initiatives where possible, so that a controller is not put through two sandboxes with two sets of conditions. (e) Direct engagement by JPDP with the major AI providers on consumer-tier training defaults for Malaysian users, which other data protection regulators in the region have done and which would help every Malaysian controller at once.	7.5; 10.4; 11.2	6(g), 9, 10

Question	Our answer	Core paras	Recs
7. Which local or international laws, standards, guidelines, frameworks or regulatory approaches should be referenced to strengthen this Framework?	Local instruments first, because what the Framework most needs is to fit with them: the ADMP Guideline (which it should cross-refer in Parts G, H and I), the DPIA and DPbD Guidelines, the DPO Guidelines, the Cross-Border Transfer Guidelines, Circulars No. 1/2025 and No. 2/2025, the Personal Data Protection Standard 2015, the National Guidelines on AI Governance and Ethics (2024), and, when enacted, the AI Governance Bill, with which the Framework should state its boundary and a one-assessment principle. International, for comparison only: the Singapore PDPC's advisory guidelines on AI recommendation and decision systems (2024) and on generative AI (July 2026); the Hong Kong PCPD's Model Personal Data Protection Framework for AI (2024) and its checklist on employees' use of generative AI (2025); the UK ICO's guidance on AI and data protection; ISO/IEC 42001 as the certifiable management-system standard relevant to due diligence; and, on three narrow points only, the EU AI Act (Recital 12 on rules-based systems, Article 9(8) on pre-defined test metrics, and Annex IV on documentation). We do not suggest the Framework follow the EU model. Act 709 is a different statute and the Framework is right to be built on it.	11.1 to 11.3	3, 10

Notes on mapping

1. Questions 1 and 3 overlap. We have answered question 1 at the level of what needs clarifying and question 3 at the level of specific drafting suggestions, so that the two answers together give the full picture without repeating each other.
2. Recommendation 11 (biometric data) answers question 2 as an additional concept and question 3 as a lifecycle control. It is the one issue in our submission that the Framework does not address at all.
3. Where a recommendation is referred to by limb (for example 6(f)), the limb is identified in the Core Submission at the end of the relevant Part.

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. Specific advice should be sought for particular circumstances.