

ANNEXURE C

Arrangements with AI Service Providers under Framework Paragraph 21.3: A Terms Review Checklist and Model Clauses

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

Why this Annexure has two parts

Paragraph 21.3 of the Framework lists seven matters that the arrangements between a data controller and an AI service provider acting as a data processor should cover. The list is sound. The difficulty is that most Malaysian controllers will never negotiate those arrangements. A company that subscribes to a global AI service accepts the provider's standard terms and, usually, a published data processing addendum. What it actually controls is the settings it chooses in the service and the records it keeps.

Part 1 is written for that controller. It is a checklist, keyed to paragraph 21.3(a) to (g), of what to look for in a provider's standard terms, where to find it, what a good answer looks like, what to do if the answer is missing or weak, and what to record. Used this way, the provider's terms and addendum, the controller's configuration, and the controller's record together make up the "appropriate arrangements" paragraph 21.3 asks for (Core paragraph 7.10 and Recommendation 6(g)).

Part 2 is written for the smaller number of cases where the controller holds the pen: a local vendor, a systems integrator, a Malaysian software product, or a custom build. It offers model clauses, keyed to the same seven matters, as a starting point for non-mandatory clauses JPDP might publish.

Both parts are offered to the drafting team as starting points and can be used, adapted or set aside. In this Annexure, "Controller" means the data controller, "Provider" means the AI service provider, "Service" means the AI system, model, functionality or service supplied, and "Act 709" means the Personal Data Protection Act 2010 as amended. Figures and terms that are for JPDP or the parties to decide are shown in square brackets.

Part 1: Terms review checklist for standard-form AI services

How to use it. Work through the rows before any personal data goes into the Service. For each row, find the term in the Provider's documents that answers the question and note where it is. Where no term answers it, follow the "if missing or weak" column. Keep the completed checklist as part of the AI Processing Record (Framework paragraph 40.4).

Where the answers usually are. Global providers typically publish, for their business and API customers: an enterprise or commercial agreement; a data processing addendum (often called a DPA); a usage or acceptable-use policy; a privacy policy; a list of sub-processors; a security or trust page; and an admin console in which the customer sets retention, training and access options. Consumer plans usually have only consumer terms and a privacy policy, and no DPA. The absence of a DPA is itself an answer: the Service is not being offered on processor terms.

Para 21.3	What to check	Where it usually is	Good answer	If missing or weak	Record
Before (a)	Is the Provider a processor at all? Do the terms say the Provider processes customer data only to provide the Service and on the customer's instructions? Do they say the Provider does not use customer inputs or outputs to train or improve its models?	DPA; enterprise agreement; the "training" or "data use" section of the privacy policy; the console setting for model training	Processor language in a DPA, and either no-training terms by default or a training setting that is off and cannot be turned on without the customer's action	If inputs may be used for training and the setting cannot be switched off, the Provider is a third party for that use and personal data should not go in without a basis under sections 6, 8 and 40 of Act 709 (Core paragraphs 7.4 and 7.5). If a switch exists, turn it off on every account and verify it	Plan type; the document and clause relied on; the training setting and the date it was checked
(a)	Nature and purpose. Do the terms limit processing to providing the Service? Is "providing the Service" defined narrowly enough (not "improving our products generally")?	DPA (scope or purpose clause); enterprise agreement	Processing limited to providing, securing and supporting the Service for the customer	Restrict use to non-personal data, or anonymise before input	The purpose clause relied on
(b)	Categories of data. Does the Provider accept personal data at all, and sensitive personal data? Some usage policies prohibit certain categories (for example health or biometric data)	Usage policy; DPA (description of processing)	Clear statement of what may be submitted; any prohibited categories listed	Do not submit prohibited categories. For sensitive personal data, including biometric data, confirm the conditions in section 40 are met before any goes in	The categories the Controller will submit and the usage-policy clause permitting them
(c)	Instructions and settings. Which settings does the Controller control: training, retention period, data region, logging, who can create accounts, whether staff can use personal accounts? Will the Provider change settings without notice?	Console; DPA (instructions clause); product documentation	The Controller can set training off, retention short, region chosen, and access limited by admin; changes to terms notified in advance	Choose the most protective available setting; if a protective setting is only on a higher plan, treat that as a cost of using the Service for personal data	Screenshots or exports of the settings chosen and the date

Para 21.3	What to check	Where it usually is	Good answer	If missing or weak	Record
(d)	Security. What measures does the Provider commit to, and is there independent evidence (a current certification or audit report)? Is data encrypted in transit and at rest? Is the Controller's data separated from other customers'?	Security or trust page; DPA (security annex); certification reports on request	Documented measures at least equal to the Personal Data Protection Standard 2015; a current independent report	If no independent evidence is available, weigh this in the risk assessment; for sensitive personal data, do not proceed without it	The security document and certification relied on and its date
(e)	Sub-processors and location. Who else processes the data, and in which countries? Is there a published list and notice of changes?	Sub-processor list; DPA (sub-processing clause); data region documentation	Published list, change notice, and a stated data region (ideally one the Controller can choose)	If the countries are unknown, the Transfer Impact Assessment cannot be done; treat as a reason not to use the Service for personal data	The list and date; the countries involved; the TIA reference (Framework paragraph 22)
(f)	Breach notification. Does the Provider commit to notify the customer of a personal data breach, within what time, and with what information?	DPA (security incident clause)	Notification "without undue delay" and within a stated period short enough for the Controller to meet the 72 hours under Circular No. 1/2025, in our view [24] hours	If the period is longer than [24] hours or unstated, note the gap in the breach response plan and shorten the Controller's own internal steps to compensate	The clause and period; the Provider's notification contact
(g)	Return and deletion. What happens to data on termination, and how long are prompts, outputs and logs kept during the service? Can the Controller delete data or shorten retention?	DPA (termination clause); retention documentation; console retention setting	Deletion on termination within a stated period; retention during service configurable or short by default	Set retention as short as the Service allows; if data cannot be deleted on request, treat as a reason not to use the Service for personal data	The retention setting chosen and the deletion commitment relied on
Rights (Framework Part G)	Data subject requests. Can the Controller retrieve, correct or delete an individual's data held in the Service, so that it can answer access and correction requests under Act 709?	Product documentation; DPA (assistance clause); console	Export, correction and deletion tools or a stated assistance commitment	If the Controller cannot retrieve an individual's data, it cannot answer an access request; weigh this before using the Service for personal data	The tool or clause relied on

One page is enough. For most small controllers the completed checklist will be a single page. The important thing is that it exists, that it is dated, and that it is reviewed when the Provider changes its terms or the Controller changes plan (Framework paragraph 23.2).

Part 2: Model clauses for negotiated arrangements

These clauses are for the case where the Controller's paper governs. They are keyed to paragraph 21.3(a) to (g), with one further clause on cooperation and audit. They also serve as the benchmark for reading Part 1: for each clause, the Part 1 question is whether the Provider's standard terms do the same work.

Para 21.3	Matter	Model clause
(a)	Nature and purpose of the processing	1. Processing. The Provider shall process personal data only to provide the Service to the Controller as described in [Schedule], and for no other purpose. The Provider shall not use personal data supplied by or on behalf of the Controller, or generated by the Service from that data, to train, retrain, fine-tune, evaluate or improve any AI model, whether its own or a third party's, unless the Controller has agreed to that use in writing and has confirmed that it holds a basis under Act 709 for it.
(b)	Categories of personal data	2. Data. The categories of personal data and of data subjects to be processed are set out in [Schedule]. The Provider shall not be required to process sensitive personal data within the meaning of Act 709, including biometric data, unless [Schedule] expressly provides for it and the Controller confirms that the conditions of section 40 of Act 709 are met.
(c)	Instructions of the Controller	3. Instructions. The Provider shall process personal data only on the Controller's documented instructions, which include this Schedule and the Controller's configuration of the Service. Where the Provider offers settings that control retention, use or training on personal data, the Provider shall apply the settings the Controller selects and shall not change them without the Controller's written agreement. If the Provider considers that an instruction would contravene Act 709, it shall inform the Controller promptly.
(d)	Measures to protect personal data	4. Security. The Provider shall implement technical and organisational measures appropriate to the risk, meeting at least the Personal Data Protection Standard 2015, including encryption of personal data in transit and at rest, logical separation of the Controller's data from other customers' data, access limited to personnel who need it and who are bound by confidentiality, logging of access, and regular testing of those measures. The Provider shall give the Controller, on request and not more than [once a year], evidence of those measures, which may be a current certification or independent assurance report.
(e)	Other processors and third parties	5. Sub-processors. The Provider shall not engage another processor or disclose personal data to any third party except as listed in [Schedule] or with the Controller's prior written agreement. The Provider shall give at least [30] days' notice of any change to that list, shall impose on each sub-processor obligations no less protective than this Schedule, and shall remain responsible to the Controller for the sub-processor's performance. Where any sub-processor processes personal data outside Malaysia, the Provider shall tell the Controller the country concerned so that the Controller can comply with section 129 of Act 709.

Para 21.3	Matter	Model clause
(f)	Security incidents and personal data breaches	6. Breach notification. The Provider shall notify the Controller of any personal data breach affecting the Controller's personal data without undue delay and in any event within [24] hours of becoming aware of it, giving the information the Controller needs to comply with section 12B of Act 709 and Circular No. 1/2025, including the time the Provider became aware, the nature of the breach, the categories and approximate number of data subjects and records affected, the AI system or model and version involved, the likely consequences, and the measures taken or proposed. The Provider shall supplement that information as it becomes available, cooperate with the Controller's investigation and notifications, and not notify data subjects or the Commissioner on the Controller's behalf unless the Controller asks it to.
(g)	Return, deletion or disposal	7. Return and deletion. On termination or expiry of the Service, or earlier on the Controller's request, the Provider shall at the Controller's option return the personal data in a commonly used electronic format or securely delete it, and shall delete remaining copies, including from backups within [the Provider's backup cycle, not exceeding 90 days], except to the extent that Act 709 or other written law requires the Provider to keep it. The Provider shall confirm deletion in writing. Personal data processed through the Service shall not be kept by the Provider for longer than is needed to provide the Service, unless the Controller instructs otherwise.
Framework Part G; Core 9.5	Cooperation and audit	8. Cooperation. The Provider shall assist the Controller in responding to data subject requests under Act 709 relating to personal data processed through the Service, including requests for access to, correction of, or deletion of personal data generated by the Service, within a time that allows the Controller to meet its statutory deadlines. The Provider shall make available the information reasonably needed to demonstrate compliance with this Schedule, including model or system documentation for the Service, and shall allow audits by the Controller or an independent auditor on reasonable notice, not more than [once a year] unless a breach or regulatory request requires otherwise.

A note on the notification window

The figure in row (f) of Part 1 and Clause 6 of Part 2 is bracketed because it is for JPDP to state (Core Recommendation 8(d)). A window of 24 hours leaves the Controller 48 hours within the 72-hour period under Circular No. 1/2025. In our experience that is the minimum a small controller needs to confirm what happened, decide whether the threshold is met, and prepare the notification.

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. It is offered to assist the drafting team and is not a substitute for terms reviewed or negotiated for a particular arrangement. Specific advice should be sought for particular circumstances.