PDPA PROGRAMME PACK · B9

Vendor and data intermediary checklist

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd. (fictional) is invented. All people are shown by role only.

Organisation	Quillmarrow Supplies Pte. Ltd. (fictional)
Document	B9 · Vendor and data intermediary checklist
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Chief Operating Officer
Label	Fictional organisation, illustrative only, not a client case study

1. What this is for

Use this checklist before appointing or renewing a vendor that will handle personal data for Quillmarrow. It helps the responsible owner understand what the vendor does, where information goes, what controls are described and what evidence remains outstanding.

A data intermediary processing personal data on Quillmarrow's behalf has protection, retention and breach-notice duties. Quillmarrow remains responsible for the personal data and should not assume that appointing a vendor transfers all of its responsibilities. The DPO should confirm how the duties apply to each arrangement with a Singapore-qualified lawyer.

The checklist supports review of G-07, G-08, G-09 and G-10. Use it alongside the B3 data inventory, B8 retention schedule and B11 breach management plan. It is not, by itself, evidence that a vendor's controls are operating or that an overseas transfer has appropriate safeguards.

2. How to use it

The business owner proposes the review, with the IT Manager coordinating technical questions and the Head of Operations, Quillmarrow's appointed DPO, overseeing personal data and transfer questions. Send the checklist before a new appointment or renewal, and repeat the review when the service, access, processing location or risk changes materially.

Before sending it, use B3 to describe the service and the relevant personal data. Ask the vendor to identify any subcontractors and locations involved, and to provide supporting documents appropriate to the service. Do not send customer databases or unnecessary personal data as part of the review.

For each answer, record:

- The question ID, response and date received.

- The person or role reviewing it and the relevant service or system.
- The supporting evidence, its location and date, or **“Not provided”**.
- The gap, proposed action, owner and target date.

Distinguish a vendor’s statement from evidence that has been reviewed. A blank answer or unavailable document stays visible as missing; do not infer that a control exists. Record unresolved actions in B2 and refer material contract or legal questions to a Singapore-qualified lawyer.

The three records below are completed as **review records**, not as proof that all questions were answered or supporting documents received. Other vendors named in B3, including Fictional PayGate, Fictional MailBurst, Fictional PeopleDesk, Fictional Helpdesk and Fictional LedgerOne, remain in scope for the checklist but are not completed in this sample.

3. Summary of DV-01 to DV-03

Vendor	Role	Overseas	Biggest gap	Next action	Owner role	Due
DV-01 Tanjung Contoh Logistics Sdn. Bhd.	Malaysia fulfilment and delivery; data intermediary for PD-11	Yes: Malaysia	The contract has a confidentiality clause but no data protection clauses. Transfer safeguards and disposal evidence are not established.	Review the arrangement and proposed transfer safeguards with a Singapore-qualified lawyer; obtain the partner’s retention and deletion arrangements for RS-20. Record evidence and open points in B2.	Head of Operations, as DPO	30 November 2026
DV-02 Fictional ShopCloud	Web-shop platform; data intermediary for relevant customer and order records	Hosting region to be confirmed	Hosting location is unknown; MFA is not in place for ShopCloud administrators.	Confirm hosting and any transfer locations, request supporting evidence, and agree an administrator MFA action with the vendor. Assess safeguards with a lawyer where relevant.	IT Manager	MFA by 13 November 2026 (G-07); hosting answer by 15 December 2026 (G-09)
DV-03 Fictional Harbour IT	Managed service provider with administrator access to Microsoft 365 and the file server	Not established	MSP administrator access has not been reviewed. Evidence of access controls and other vendor safeguards is not established.	Review named administrator accounts, permissions and access needs; obtain and assess available control evidence. Record any removals or changes separately.	IT Manager	13 November 2026 (G-07)

These dates are proposed targets. The DPO should review outstanding answers and evidence with each owner and escalate unresolved risks to the COO. A questionnaire response alone does not close an action.

4. Contract points to raise with your lawyer

The following are discussion points for a Singapore-qualified lawyer, **not legal drafting**. The contract should reflect the actual service, data and locations rather than relying on a generic clause.

1. **Purpose and instructions.** Define the service, the personal data involved and the permitted purposes. Address how Quillmarrow gives instructions and how the vendor handles requests to use data for another purpose.
2. **Security measures.** Specify proportionate technical and organisational measures, including access controls, administrator privileges, authentication, logging and secure transmission where relevant. Agree how material changes are communicated.
3. **Breach notice to Quillmarrow.** A data intermediary processing on Quillmarrow's behalf must notify Quillmarrow without undue delay after it has credible grounds to believe a breach occurred. Agree the contact route, information to provide and how updates will be supplied.

4. **Breach response cooperation.** Require practical assistance with containment, investigation, preservation of relevant evidence and follow-up. Coordinate these arrangements with B11; notification to Quillmarrow is separate from Quillmarrow's own assessment and notification decision.
5. **Sub-processors.** Define whether the vendor may appoint another processor, what approval or notice is needed, and how equivalent obligations and oversight will be arranged.
6. **Locations and transfers.** Identify where data is accessed, stored and processed, and how changes will be notified. For overseas transfers, ask the lawyer to assess appropriate safeguards; the ASEAN Model Contractual Clauses may be one option.
7. **Retention and end of service.** Agree retention instructions consistent with confirmed B8 decisions, the return or secure deletion of information at the end of service, treatment of backups, permitted exceptions and evidence of completion.
8. **Audit and evidence rights.** Agree what assurance documents, audit access or independent reports Quillmarrow may request, how often they will be reviewed and how identified gaps will be addressed.
9. **Staff confidentiality and access.** Address confidentiality commitments, access limited to authorised personnel, prompt removal of unnecessary access and the vendor's responsibility for its personnel.
10. **Access and correction assistance.** Set out how the vendor will forward requests and assist Quillmarrow to locate, provide or correct information in time for the B7 process. Clarify responsibilities where a request is received directly by the vendor.
11. **Changes, termination and unresolved issues.** Agree how changes to the service or risk are reviewed, how Quillmarrow can raise and track concerns, and what happens to access and data when the arrangement ends.

5. Decision after the review

The checklist ends in a decision, recorded by the DPO and approved by the COO. The three options are: **continue** (answers and evidence are adequate), **continue with conditions** (named actions and a date, tracked in B2), or **stop or replace** (the risk cannot be brought to an acceptable level).

Vendor	Proposed decision now	Conditions	Decision owner
DV-01 Tanjung Contoh Logistics	Continue with conditions	Data protection terms and transfer safeguards agreed after legal review; RS-20 deletion confirmed in writing; requests forwarded to Quillmarrow promptly (see B7, AR-06).	COO, on the DPO's recommendation
DV-02 Fictional ShopCloud	Continue with conditions	Admin MFA switched on; hosting region confirmed in writing and checked with B10.	COO, on the DPO's recommendation
DV-03 Fictional Harbour IT	Continue with conditions	Named admin list reviewed and trimmed; breach notice route agreed so that B11 can start on time.	COO, on the DPO's recommendation

The decision, the evidence relied on and any open conditions are recorded against the vendor in B2 (G-07 or G-09). A vendor that has not answered by the due date is escalated to the COO, not quietly carried forward.

The 18-question vendor checklist follows.

Evidence summary

Vendor	Evidence provided	Partial	Not provided	Not applicable
DV-01 Tanjung Contoh Logistics (Malaysia)	0	6	12	0
DV-02 Fictional ShopCloud	0	3	15	0
DV-03 Fictional Harbour IT	0	3	15	0

Role and data

Q	Question and evidence requested	DV-01 Tanjung Contoh Logistics (Malaysia)	DV-02 Fictional ShopCloud	DV-03 Fictional Harbour IT
VQ-01	**What services do you provide, and what personal data do you receive, access or otherwise process for Quillmarrow?** Evidence: Service description, data-flow diagram or processing schedule identifying data, individuals and purposes.	**Partial.** Case-file report: provides Malaysia fulfilment and delivery and receives order and delivery data. Supporting data-flow or processing documents were not supplied.	**Partial.** Case-file report: provides the web-shop platform and is a data intermediary. Data categories and processing details were not supplied.	**Partial.** Case-file report: provides IT support and has administrator access to Microsoft 365 and the file server. Data-access scope was not supplied.
VQ-02	**Do you process personal data only on Quillmarrow's documented instructions, and how are those instructions recorded?** Evidence: Processing instructions, service terms or operating procedure showing how instructions are received and followed.	**Not provided.** Not established in the case file; instructions and supporting documents were not supplied.	**Not provided.** Not established in the case file; instructions and supporting documents were not supplied.	**Not provided.** Not established in the case file; instructions and supporting documents were not supplied.
VQ-03	**What confidentiality and data-protection training do staff with access to Quillmarrow data receive?** Evidence: Training materials, completion records and confidentiality requirements for relevant staff.	**Not provided.** Not established in the case file; training and confidentiality evidence were not supplied.	**Not provided.** Not established in the case file; training and confidentiality evidence were not supplied.	**Not provided.** Not established in the case file; training and confidentiality evidence were not supplied.

Security and access

Q	Question and evidence requested	DV-01 Tanjung Contoh Logistics (Malaysia)	DV-02 Fictional ShopCloud	DV-03 Fictional Harbour IT
VQ-04	**What technical and organisational safeguards protect Quillmarrow data against unauthorised access, loss or disclosure?** Evidence: Current security policy or control summary, relevant assurance reports and remediation records.	**Not provided.** Not established in the case file; security-control evidence was not supplied.	**Not provided.** Not established in the case file; security-control evidence was not supplied.	**Not provided.** Not established in the case file; security-control evidence was not supplied.
VQ-05	**How is access to Quillmarrow data granted, restricted, logged and removed?** Evidence: Access-control procedure, sample access records and joiner, mover and leaver controls.	**Not provided.** Not established in the case file; access-control and logging evidence was not supplied.	**Not provided.** Not established in the case file; access-control and logging evidence was not supplied.	**Partial.** Case-file report: administrator access to Microsoft 365 and the file server has not been reviewed. Access lists, review records and removal controls were not supplied.
VQ-06	**Is multi-factor authentication enabled for privileged and remote access to systems containing Quillmarrow data?** Evidence: Configuration evidence covering privileged and remote accounts, exceptions and remediation plans.	**Not provided.** Not established in the case file; authentication configuration evidence was not supplied.	**Partial.** Case-file report: MFA is not enabled on the Fictional ShopCloud admin account. Configuration evidence and remediation plan were not supplied.	**Not provided.** Not established in the case file; authentication configuration evidence was not supplied.

Breach and incidents

Q	Question and evidence requested	DV-01 Tanjung Contoh Logistics (Malaysia)	DV-02 Fictional ShopCloud	DV-03 Fictional Harbour IT
VQ-07	**How do you identify, contain, investigate and document a suspected security or personal-data incident?** Evidence: Incident-response procedure, escalation contacts and a suitably redacted incident record or exercise evidence.	**Not provided.** Not established in the case file; incident-response evidence was not supplied.	**Not provided.** Not established in the case file; incident-response evidence was not supplied.	**Not provided.** Not established in the case file; incident-response evidence was not supplied.
VQ-08	**How and when will you notify Quillmarrow after discovering a suspected breach involving its data?** Evidence: Contractual notification commitment, incident escalation procedure and contact route.	**Not provided.** Not established in the case file; notification terms and procedure were not supplied.	**Not provided.** Not established in the case file; notification terms and procedure were not supplied.	**Not provided.** Not established in the case file; notification terms and procedure were not supplied.
VQ-09	**What incident records, investigation findings and corrective actions can you provide to support Quillmarrow's assessment?** Evidence: Incident register fields, investigation and evidence-preservation process, and corrective-action tracking procedure.	**Not provided.** Not established in the case file; incident record and corrective-action evidence were not supplied.	**Not provided.** Not established in the case file; incident record and corrective-action evidence were not supplied.	**Not provided.** Not established in the case file; incident record and corrective-action evidence were not supplied.

Retention and return

Q	Question and evidence requested	DV-01 Tanjung Contoh Logistics (Malaysia)	DV-02 Fictional ShopCloud	DV-03 Fictional Harbour IT
VQ-10	**How long do you retain Quillmarrow data, and how are retention and deletion periods applied?** Evidence: Retention schedule, system settings and deletion or expiry evidence for relevant data.	**Not provided.** Not established in the case file; partner retention schedule and deletion settings were not supplied.	**Not provided.** Not established in the case file; platform retention schedule and deletion settings were not supplied.	**Not provided.** Not established in the case file; MSP retention schedule and deletion settings were not supplied.
VQ-11	**At the end of the service or on request, how do you return or securely delete Quillmarrow data, including copies?** Evidence: Return and deletion procedure, backup treatment, and sample deletion or return confirmation.	**Not provided.** Not established in the case file; return, deletion and backup arrangements were not supplied.	**Not provided.** Not established in the case file; return, deletion and backup arrangements were not supplied.	**Not provided.** Not established in the case file; return, deletion and backup arrangements were not supplied.
VQ-12	**Can you provide evidence that Quillmarrow data has been returned or deleted, and explain any data that cannot yet be removed?** Evidence: Deletion certificate or equivalent record, exceptions and the planned date for their removal.	**Not provided.** Not established in the case file; deletion evidence and exception details were not supplied.	**Not provided.** Not established in the case file; deletion evidence and exception details were not supplied.	**Not provided.** Not established in the case file; deletion evidence and exception details were not supplied.

Sub-processors and location

Q	Question and evidence requested	DV-01 Tanjung Contoh Logistics (Malaysia)	DV-02 Fictional ShopCloud	DV-03 Fictional Harbour IT
VQ-13	**Do you use sub-processors to deliver the service, and how are they approved and monitored?** Evidence: Current sub-processor list, service locations, due-diligence records and change-notification process.	**Not provided.** Not established in the case file; sub-processor information and monitoring evidence were not supplied.	**Not provided.** Not established in the case file; sub-processor information and monitoring evidence were not supplied.	**Not provided.** Not established in the case file; sub-processor information and monitoring evidence were not supplied.
VQ-14	**In which countries or regions are Quillmarrow data stored, accessed or otherwise processed?** Evidence: Current data-location schedule covering primary hosting, backups, support access and transfers.	**Partial.** Case-file report: DV-01 operates in Johor, Malaysia and receives order and delivery data. Storage, backup and support-access locations were not supplied.	**Partial.** Case-file report: the hosting region is to be confirmed. No location evidence was supplied.	**Partial.** Case-file report: DV-03 has administrator access to Microsoft 365 and the file server. Its processing and access locations were not supplied.
VQ-15	**What safeguards apply to any overseas transfer or overseas access involving Quillmarrow data?** Evidence: Transfer assessment, applicable contractual safeguards, access locations and supporting transfer documentation.	**Partial.** Case-file report: data is transferred to the Malaysia partner; the reported contract has a confidentiality clause but no data-protection clauses. Transfer assessment and safeguards evidence were not supplied.	**Not provided.** Hosting region is to be confirmed; overseas hosting or access and any transfer safeguards are not established in the case file.	**Not provided.** Overseas access or transfer arrangements are not established in the case file; supporting evidence was not supplied.

Contract

Q	Question and evidence requested	DV-01 Tanjung Contoh Logistics (Malaysia)	DV-02 Fictional ShopCloud	DV-03 Fictional Harbour IT
VQ-16	**Does the written agreement define the service, data-processing instructions, confidentiality and security obligations?** Evidence: Executed agreement and relevant schedules covering services, processing, confidentiality and security.	**Partial.** Case-file report: the contract includes a confidentiality clause but no data-protection clauses. The contract itself and other terms were not supplied.	**Not provided.** Contract terms were not supplied; the relevant obligations are not established in the case file.	**Not provided.** Contract terms were not supplied; the relevant obligations are not established in the case file.
VQ-17	**Does the agreement require prompt breach notification, cooperation with investigations and support for data-subject requests?** Evidence: Executed contract clauses and operational procedure covering notification, cooperation and request support.	**Partial.** Case-file report identifies a confidentiality clause but no data-protection clauses; breach and request-support terms were not supplied.	**Not provided.** Contract terms and supporting procedures were not supplied.	**Not provided.** Contract terms and supporting procedures were not supplied.
VQ-18	**Does the agreement cover sub-processor changes, retention and deletion, audits or assurance, and assistance with overseas-transfer safeguards?** Evidence: Executed contract and schedules covering sub-processors, retention, deletion, assurance and any transfer safeguards.	**Partial.** Case-file report: the contract has a confidentiality clause but no data-protection clauses. Terms for sub-processors, retention, deletion, assurance and transfer safeguards were not supplied.	**Not provided.** Contract terms and hosting-region evidence were not supplied; transfer and related safeguards remain unclear.	**Not provided.** Contract terms, access-review commitments and assurance evidence were not supplied.

About this sample

Fictional organisation, illustrative only, not a client case study. Quillmarrow Supplies Pte. Ltd., its people, vendors, findings and dates are invented. Nothing in this document reports a client result.

I personally review and sign off every deliverable. You appoint your own DPO. I support them.

This is practical compliance support, not legal advice. For legal advice, use a Singapore-qualified lawyer.

What's not included

- Acting as your DPO. You appoint your own DPO; I prepare the handover and can support them separately.
- Legal advice, legal contract drafting, representation or a guarantee of compliance.
- Forensic investigation, penetration testing, security engineering or implementing changes in live systems.
- A detailed AI governance review or ISO/IEC 42001 readiness check unless separately scoped.
- Ongoing document upkeep after handover, unless agreed through monthly DPO support.
- Healthcare-sector work or on-site delivery.

Questions about this sample: DM @alewyl1 on X, or ask for a free intro call (coffee chat).