PDPA PROGRAMME PACK · B2

Gap review and action plan

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	B2 · Gap review and action plan
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Managing Director
Label	Fictional organisation, illustrative only, not a client case study

1. Summary for management

Quillmarrow has appointed the Head of Operations as its Data Protection Officer (DPO), but several core documents and repeatable processes still need to be put in place. The pack rates three areas Red, seven Amber and one Green. The three Red areas are **G-04 Notification**, **G-08 Retention limitation** and **G-10 Data breach notification**. They come first because people are not consistently told how their data will be used, records are generally kept without a retention schedule, and staff do not yet have a documented breach assessment and decision process. These gaps affect several collection points and systems, and the SharePoint near-miss illustrates why a clear escalation route matters. There are also important Amber actions concerning marketing consent, access requests, system access and overseas transfers. Some practices are already working: order-related checkout consent is reported as satisfactory, B2B details are checked at onboarding and annually, and Microsoft 365 has multi-factor authentication. The ratings are illustrative working priorities, not findings that Quillmarrow does or does not comply with the law.

2. How the review was done

The programme uses interviews with relevant role holders, review of available documents and system walk-throughs using descriptions and screenshots with personal data masked. The intended interviewees include the DPO, COO, IT Manager, Head of Customer Service, Head of Marketing, HR Manager and other owners of the processes described in B3. No customer database was received, and no client personal data was put into AI tools.

This narrative reflects the supplied case facts. Where the case file reports a practice, it is described as reported; it does not establish that the reviewer independently tested a live configuration or received every supporting record. The detailed tracker should identify the evidence available for each finding and distinguish an unverified description from a reviewed document or screenshot.

The ratings are working labels for management:

- **Red:** a material document or process is absent, or the reported gap needs early coordinated attention.
- **Amber:** a practice exists or is partly understood, but a material gap, inconsistency or evidence question remains.
- **Green:** the reported practice is established for this review area, subject to the evidence and review scope.

Priority is separate from the RAG rating. **P1** means start now (target within about two weeks), **P2** within 60 days, and **P3** within 90 days as routine maintenance or confirmation. The dates in the heat summary and the tracker are the same dates; the tracker is the master copy. These labels are planning aids, not legal conclusions. Proposed target dates below are for Quillmarrow to agree; they are not evidence that an action has been completed.

The relevant references are the *Personal Data Protection Act 2012 (PDPA)*, the *PDPC Advisory Guidelines on Key Concepts in the PDPA*, the *PDPC Guide on Managing and Notifying Data Breaches under the PDPA*, and the *PDPC Advisory Guidelines on the Do Not Call Provisions*. Questions about legal requirements and proposed wording should be confirmed with a Singapore-qualified lawyer.

3. Heat summary

Area	RAG	Priority	Owner role	Target date
G-01 Accountability	Amber	P2 within 60 days	Head of Operations, appointed DPO	30 Nov 2026
G-02 Consent	Amber	P1 now	Head of Marketing	13 Nov 2026
G-03 Purpose limitation	Amber	P2 within 60 days	Showroom Supervisor	15 Dec 2026
G-04 Notification	Red	P1 now	Head of Operations, appointed DPO	13 Nov 2026
G-05 Access and correction	Amber	P1 now	Head of Customer Service	13 Nov 2026
G-06 Accuracy	Green	P3 within 90 days	Sales Manager	29 Jan 2027
G-07 Protection	Amber	P1 now	IT Manager	13 Nov 2026
G-08 Retention limitation	Red	P1 now	Head of Operations, appointed DPO	15 Dec 2026
G-09 Transfer limitation	Amber	P2 within 60 days	Head of Operations, appointed DPO	15 Dec 2026
G-10 Data breach notification	Red	P1 now	Head of Operations, appointed DPO	13 Nov 2026
G-11 Do Not Call provisions	Amber	P1 now	Head of Marketing	13 Nov 2026

The DPO coordinates the programme; each listed owner is responsible for the proposed action in their area. The MD approves the data protection policy, B11 breach management plan and final pack. The COO is the programme sponsor and should resolve cross-team dependencies.

The dates are proposed completion or decision targets. If a supplier or adviser cannot provide required evidence by a target, the owner should record the dependency, interim measure and revised date rather than close the action without evidence.

4. Top five actions in order

1. Establish the breach response and decision process

Owner: Head of Operations, appointed DPO, with the IT Manager and Head of Customer Service.
Pack document: B11 data breach management plan and playbook, with the INC-2026-07 worked example in B11 section 8 and the staff briefing in B15.
Target: 13 November 2026 (G-10).

The near-miss was handled by email, and the case file records no breach plan, assessment form or decision log. The DPO should agree an escalation route, response roles and deputies, and ensure the assessment of facts is kept separate from the MD's notification decision. The IT Manager should identify how relevant logs can be preserved and how Fictional Harbour IT will be contacted.

Evidence of closure: MD-approved B11; completed contact and deputy list; a usable assessment form and separate decision record; and confirmation that response owners have received the plan. Filing a draft alone does not close G-10. Record any untested technical or supplier dependency.

2. Replace missing and outdated collection-point notices

Owner: Head of Operations, appointed DPO, with the Head of Marketing, HR Manager and Showroom Supervisor.
Pack document: B4 privacy notices (website, B2B account form, job applications, showroom sign-up and CCTV sign).
Target: 13 November 2026 (G-04).

The website statement dates from 2019, and no notice is recorded for the job-application form, showroom sign-up or CCTV signage. Use B3 to check what information is collected and why, including PD-09, PD-13 and PD-15. Draft notices should be relevant to each collection point and consistent with actual practices.

Evidence of closure: approved wording for each relevant point; screenshots or photographs showing publication or display; and a record of the owner and review date. Confirm legal wording with a Singapore-qualified lawyer. If a notice is approved but not yet displayed, keep the implementation action open.

3. Agree retention decisions and a disposal plan

Owner: Head of Operations, appointed DPO, with the Finance Director, HR Manager and IT Manager.
Pack document: B8 retention schedule, linked to B3.
Target: 15 December 2026 (G-08).

The case file reports no retention schedule and indefinite retention generally. Quillmarrow should decide what to keep, why, for how long, who approves exceptions and how disposal will be evidenced. Confirm whether the reported approximately 30-day CCTV overwrite is actually configured; do not treat the report as a verified setting.

Evidence of closure: management-approved decisions for RS-01 to RS-20; assigned owners and disposal methods; a documented implementation plan; and, where a disposal has occurred, an appropriate record of completion. For accounting and tax records, confirm periods driven by law with your accountant or lawyer. RS-20 also requires agreement and evidence from DV-01.

4. Correct marketing choices and prepare the DNC process

Owner: Head of Marketing, supported by the Sales Manager and DPO.
Pack documents: B3 inventory, B6 consent and withdrawal procedures, and B12 DNC checklist.
Target: 13 November 2026 (G-02 and G-11), and in any case before the planned telemarketing campaign starts.

Review the pre-ticked marketing consent box on the B2B account form and the absence of consent records for showroom sign-ups. For PD-08, PD-09 and PD-10, establish what choices were recorded, how withdrawal is handled and what can be supported by evidence. Prepare a telemarketing check and record process, including standard sender details.

Evidence of closure: approved revised forms and wording; screenshots or samples showing the revised collection method; a documented withdrawal route; and a campaign checklist with a DNC check **within the validity period set by the PDPC (confirm the current period)**. Obtain legal advice on the proposed approach. Do not treat an unrecorded choice as evidenced consent.

5. Restrict access and resolve priority supplier questions

Owner: IT Manager for access controls; Head of Operations as DPO for vendor and transfer decisions.
Pack documents: B2 tracker, B3 inventory and B9 vendor due-diligence questionnaire.
Target: 13 November 2026 for the access review (G-07); 15 December 2026 for the supplier and transfer decisions (G-09), using B10 for the transfer check.

Review SharePoint link-sharing arrangements after the near-miss, the reported absence of MFA on Fictional ShopCloud administration, and Fictional Harbour IT's administrator access. For DV-01, seek the contract and transfer safeguards relevant to PD-11. For DV-02, obtain the hosting region and any relevant access locations. Do not assume that a confidentiality clause alone answers all transfer questions.

Evidence of closure: reviewed administrator access list and decisions; masked configuration evidence for agreed changes; vendor responses and supporting documents; and a documented transfer decision after legal review where needed. An unresolved supplier response remains open in G-07 or G-09 even if a questionnaire has been sent.

5. Evidence still missing

The following evidence is **not established as received in the case file**. The DPO should request or locate it; the case file does not establish that every item was previously requested.

- DV-02 Fictional ShopCloud's hosting region, backup and support-access locations, supported by supplier documentation.
- A current DV-03 Fictional Harbour IT administrator access list, the last access review, and evidence of removal or approval of access.
- Masked evidence of the Fictional ShopCloud administrator MFA setting and any remediation.
- The DV-01 Malaysia contract and any data-protection or transfer annex, together with the partner's retention and deletion arrangements for RS-20.
- The current SharePoint sharing configuration, the retained log export for INC-2026-07 and evidence of any subsequent restriction.
- Published or displayed notices for job applicants, showroom sign-ups and CCTV, if they exist.
- Consent records for showroom sign-ups and evidence of how B2B marketing preferences and withdrawals are recorded.
- A verified CCTV overwrite setting and an owner-approved retention decision for RS-09.
- Existing request records supporting handling times, identity checks and decisions, including the 41-day request represented by AR-02.

The detailed tracker should link each item to its request owner and date. Absence from this list does not imply that other evidence has been reviewed.

6. Decisions needed from management

1. **Approve the policy, breach plan and final pack.** The MD should decide whether the documents are ready for approval and record any conditions or open actions.
2. **Confirm action owners and target dates.** The COO should resolve cross-team ownership and dependencies; the DPO should update B2.
3. **Approve notice and marketing changes.** The DPO and Head of Marketing should recommend wording and implementation; the MD should resolve material policy choices after legal review where appropriate.
4. **Approve retention decisions and implementation.** The DPO should coordinate owners' proposals; the Finance Director should obtain accountant or lawyer confirmation for accounting and tax requirements before the relevant decisions are finalised.
5. **Decide supplier and transfer next steps.** The DPO should review DV-01 and DV-02 evidence with the relevant owners and seek advice from a Singapore-qualified lawyer on safeguards and unresolved questions.
6. **Confirm the telemarketing launch gate.** The Head of Marketing should not treat the campaign checklist as complete until the DNC process, sender details and supporting records have been agreed and reviewed.

7. Interim measures until actions close

Some actions will take weeks. Until they close, the owners should apply these holding measures and record them in the tracker:

Gap	Interim measure	Owner role
G-10	Any suspected breach goes straight to the DPO by phone and email; the DPO starts the B11 assessment form the same day.	Head of Operations, appointed DPO
G-07	External SharePoint sharing links are restricted to named people while the access review runs.	IT Manager
G-02, G-11	No telemarketing calls or messages go out until B6 and B12 are approved.	Head of Marketing
G-08	No bulk deletion until B8 decisions are approved, so that nothing needed for an open request or incident is lost.	Head of Operations, appointed DPO
G-04	The 2019 website statement stays up but is flagged for replacement; no new collection form goes live without a B4 notice.	Head of Operations, appointed DPO

8. Keeping the tracker live

The DPO owns B2 after handover. Each action owner updates their item with progress, evidence, dependencies and a proposed revised date where necessary. The DPO should review the tracker **monthly**, challenge overdue or unsupported closures, and coordinate changes to B3, B8, B9 and B11 when the underlying process changes.

The DPO should report to the MD **quarterly**, highlighting overdue P1 actions, decisions required, new incidents and supplier dependencies. The COO should help resolve cross-functional blockers. Retain evidence of closure alongside the relevant tracker entry; a status change without supporting evidence is not verification.

The full tracker follows.

Gap tracker, part 1: what we found

ID	Area	RAG	Current state	Gap
G-01	Accountability	Amber	The Head of Operations has been appointed as DPO. The review found that the DPO contact has not yet been published and no written data protection policy was supplied.	The policy, published contact, complaints process and staff communication are not evidenced.
G-02	Consent	Amber	The web-shop checkout consent for orders was reported as satisfactory. The B2B account form has a pre-ticked marketing consent box, and no consent records were supplied for showroom sign-ups.	The B2B marketing choice needs correction and Quillmarrow needs evidence of showroom sign-up choices and records.
G-03	Purpose limitation	Amber	The review found that recorded purposes were broadly reasonable. The supplied case facts also state that CCTV was used once in a staff timekeeping dispute, outside its stated purpose.	The CCTV purpose, access and escalation process do not show how out-of-purpose use will be prevented or reviewed.
G-04	Notification	Red	The website has a generic privacy statement dated 2019. No privacy notice was supplied for the job application form, showroom sign-up or CCTV signage.	People are not provided with current, channel-specific information at these collection points.
G-05	Access and correction	Amber	Customer Service handles requests ad hoc and no request log was supplied. One request took 41 days; six sample request scenarios, AR-01 to AR-06, identify web-shop, employee, B2B, CCTV and partner-forwarded requests.	There is no consistent intake, tracking, escalation or response evidence against the organisation's stated target.
G-06	Accuracy	Green	B2B account details are verified at onboarding. Sales conducts an annual check, as reported in the supplied review facts.	The review did not receive records demonstrating the annual checks or how corrections are carried through relevant systems.
G-07	Protection	Amber	A SharePoint folder containing customer records was link-shared to anyone with the link for two days, as described in the breach scenario. Microsoft 365 has MFA, but Fictional ShopCloud admin does not; Fictional Harbour IT admin access has not been reviewed.	The link-sharing event highlights exposure risk, while ShopCloud admin MFA and review of MSP privileged access remain open.
G-08	Retention limitation	Red	No retention schedule was supplied and the case facts state that records are kept indefinitely. CCTV is reported by Quillmarrow to be overwritten at about 30 days.	Retention and disposal decisions are missing for the record types in RS-01 to RS-20; accounting and tax periods need confirmation with an accountant or lawyer.
G-09	Transfer limitation	Amber	DV-01 receives Malaysia delivery data under a contract with a confidentiality clause but no data protection clauses. Fictional ShopCloud's hosting region is to be confirmed.	Transfer safeguards and the platform's hosting location are not evidenced; the contract and processing arrangements need review.
G-10	Data breach notification	Red	No breach plan, assessment form or decision log was supplied. INC-2026-07 was handled by email; the case facts separately record its assessment and the MD and DPO's notification decision.	Quillmarrow lacks a documented C.A.R.E. response route and consistent records separating assessment facts from the notification decision.
G-11	Do Not Call (DNC) provisions	Amber	A telemarketing campaign to SME owners is planned. No DNC register-check process was supplied, and sender details are not standardised.	The campaign lacks a documented check, suppression and sender-identification process before contact.

Gap tracker, part 2: actions, owners and evidence

ID	Priority	Action	Owner role	Evidence to close	Target date	Status
G-01	P2 within 60 days	Adopt the data protection policy, publish the DPO contact and document the complaints process; update B2.	Head of Operations	MD-approved policy, website capture showing dpo@quillmarrow.example, and documented complaints process.	30 Nov 2026	Open
G-02	P1 now	Remove the pre-ticked marketing box, establish an affirmative consent record for showroom sign-ups and update B2.	Head of Marketing	Updated B2B form, showroom sign-up process and sample consent records showing the person's choice and its source.	13 Nov 2026	Open
G-03	P2 within 60 days	Document permitted CCTV purposes and access, prohibit unrelated use unless reviewed and authorised, and record the change in B2.	Showroom Supervisor	Approved CCTV purpose and access procedure, staff communication record and documented approval route for exceptional use.	15 Dec 2026	Open
G-04	P1 now	Replace the website statement and prepare notices for job applicants, showroom sign-ups and CCTV; record the work in B2.	Head of Operations	Approved notices and dated screenshots or copies showing publication at each specified collection point.	13 Nov 2026	Open
G-05	P1 now	Adopt the access and correction procedure, log the AR-01 to AR-06 scenarios and train receiving teams; update B2.	Head of Customer Service	Approved procedure, request log template, completed scenario walkthroughs and staff briefing record.	13 Nov 2026	Open
G-06	P3 within 90 days	Retain evidence of the Sales verification cycle and document how corrections are reflected in relevant records; update B2.	Sales Manager	Dated verification record and documented correction procedure or sample completed correction record.	29 Jan 2027	Open
G-07	P1 now	Review external-link settings and privileged access, enable MFA for ShopCloud admin where available, and record remediation in B2 and B11.	IT Manager	Dated access review, ShopCloud admin MFA configuration evidence, SharePoint sharing-control evidence and remediation record linked to B11.	13 Nov 2026	Open
G-08	P1 now	Complete and approve B8, assigning a justified retention decision and disposal method for each RS record type, with accounting and tax periods flagged for confirmation.	Head of Operations	Approved B8 schedule covering RS-01 to RS-20, with owners, disposal methods and documented accountant or lawyer confirmation where relevant.	15 Dec 2026	Open
G-09	P2 within 60 days	Confirm Fictional ShopCloud's hosting region and review DV-01 terms and transfer safeguards, documenting the outcome and any agreed measures in B2.	Head of Operations	Written ShopCloud hosting-region confirmation and documented DV-01 contract review with agreed transfer safeguards or recorded unresolved issues.	15 Dec 2026	Open
G-10	P1 now	Adopt B11, including the assessment form, separate decision log, escalation route and roles for intermediary reports; test it using INC-2026-07.	Head of Operations	MD-approved B11, completed tabletop exercise record using INC-2026-07 and logged corrective actions.	13 Nov 2026	Open
G-11	P1 now	Document the campaign DNC check and suppression process, standardise sender details and record the check in B2 before calls begin.	Head of Marketing	Approved campaign procedure, standard sender script and a sample check record showing the check was made within the validity period set by the PDPC (confirm the current period).	13 Nov 2026	Open

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).