PDPA PROGRAMME PACK · B16

DPO handover pack

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	B16 · DPO handover pack
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. What you are taking over

As Head of Operations, you are Quillmarrow's appointed Data Protection Officer (DPO) and the day-to-day owner of its data protection programme. The COO is the programme sponsor. The Managing Director (MD) approves the data protection policy, breach management plan and final pack.

Quillmarrow has appointed its own DPO. The external reviewer who prepared this pack supports the DPO, is not the DPO, and does not take over Quillmarrow's decisions or legal responsibilities. Nothing in this pack is legal advice or a statement that Quillmarrow complies with the PDPA.

This handover brings together the documents, open actions and recurring work needed to maintain the programme. It is an illustrative working pack, not evidence that the proposed controls have been approved or implemented. In particular:

- The DPO's business contact has not yet been published under **G-01**.
- Notices, consent records and the marketing process need work under **G-02**, **G-04** and **G-11**.
- The retention schedule contains decisions for Quillmarrow to confirm under **G-08**.
- Vendor safeguards, the Fictional ShopCloud hosting region and administrator-access checks remain open under **G-07** and **G-09**.
- The breach plan and associated procedures need approval and implementation under **G-10**.

Use **B2** as the action tracker and **B3** as the personal data inventory. Assign an owner, target date and evidence for each action. Escalate missed dates or decisions that need authority rather than marking an action complete because a document has been drafted.

2. Document index

The SharePoint paths below are **proposed fictional locations**, not verified file locations. The DPO and IT Manager should confirm the actual library, permissions, file names and links before issuing the handover.

"Awaiting MD approval" below is a **working handover status**, not evidence that a document has been submitted to the MD. Documents marked for lawyer review may also need MD approval as part of the final pack. No item is shown as approved without evidence.

ID	Document or scope	Owner role	Approver	Working status	Proposed review cycle	Proposed fictional SharePoint location
B1	Programme scope sheet	DPO	MD, as part of final pack	Awaiting MD approval	Annually and after a material change	`SharePoint / Data Protection / B1`

ID	Document or scope	Owner role	Approver	Working status	Proposed review cycle	Proposed fictional SharePoint location
B2	Gap review and action plan	DPO	MD, as part of final pack	Awaiting MD approval	Monthly until actions close; then quarterly	`SharePoint / Data Protection / B2`
B3	Personal data inventory and data flow map	DPO, with department heads	MD, as part of final pack	Awaiting MD approval	Quarterly and before a material new use	`SharePoint / Data Protection / B3`
B4	Privacy notices	DPO, with relevant department heads	MD, as part of final pack	Draft for lawyer review	Annually and when collection or purposes change	`SharePoint / Data Protection / B4`
B5	Internal data protection policy	DPO	MD	Awaiting MD approval	Annually and after a material change	`SharePoint / Data Protection / B5`
B6	Consent and withdrawal procedures	DPO, with Head of Marketing	MD, as part of final pack	Draft for lawyer review	Annually and when forms or purposes change	`SharePoint / Data Protection / B6`
B7	Access and correction procedure and log	DPO, with Head of Customer Service and HR Manager	MD, as part of final pack	Draft for lawyer review	Annually and after a material issue	`SharePoint / Data Protection / B7`
B8	Retention schedule	DPO, with record owners	MD, as part of final pack	Draft for lawyer review	Annually and when record needs change	`SharePoint / Data Protection / B8`
B9	Vendor and data intermediary checklist	DPO, with IT Manager	MD, as part of final pack	Awaiting MD approval	Annually and before a material vendor change	`SharePoint / Data Protection / B9`
B10	Overseas transfer checklist	DPO	MD, as part of final pack	Draft for lawyer review	Annually and when the transfer changes	`SharePoint / Data Protection / B10`
B11	Data breach management plan	DPO, with IT Manager	MD	Awaiting MD approval	Annually and after an incident or exercise	`SharePoint / Data Protection / B11`
B12	DNC checklist and process	Head of Marketing, with DPO	MD, as part of final pack	Draft for lawyer review	Before campaigns and at least annually	`SharePoint / Data Protection / B12`
B13	DPIA template, with a worked example	COO, with DPO	MD, as part of final pack; COO for the proposed operational decision	Awaiting MD approval	Before launch and after material changes	`SharePoint / Data Protection / B13`
B14	Basic AI-use policy	COO	MD	Awaiting MD approval	Annually and when approved uses change	`SharePoint / Data Protection / B14`
B15	Remote staff briefing: outline and speaker notes	DPO, with HR Manager	MD, as part of final pack	Awaiting MD approval	Annually and when procedures change	`SharePoint / Data Protection / B15`
B16	DPO handover pack	DPO	MD, as part of final pack	Awaiting MD approval	Quarterly during the first year; then annually	`SharePoint / Data Protection / B16`

Before circulating the pack, the DPO should reconcile this index against the actual B1–B16 files and approval records. The proposed review cycles are management practices, not statutory periods. Keep drafts and approved versions distinguishable, with access limited to people who need them.

3. Responsibilities

The table proposes how the programme will operate after handover. **R** means responsible for doing the work; **A** means accountable for the outcome; **C** means consulted; and **I** means informed. An activity can have more than one R, but should have one A. “Department heads” includes the relevant functional role, such as the Head of Marketing, HR Manager or Head of Customer Service.

Activity	MD	COO	DPO	Department heads	IT Manager
Prepare and maintain notices	I	C	A	R	C
Maintain consent records and respond to withdrawals	I	I	A	R	C
Handle access and correction requests	I	I	A	R	C
Agree and carry out retention clean-ups	I	C	A	R	R
Perform vendor checks	I	C	A	R	R
Review overseas transfers and safeguards	I	C	A	R	R
Respond to a suspected breach	A	C	R	R	R
Carry out DNC checks before campaigns	I	I	A	R	C
Arrange and record staff training	I	C	A	R	C
Report programme status to the MD	I	C	A/R	C	C

For a breach, staff report promptly and the DPO coordinates the assessment; the MD and DPO record the notification decision as described in B11. The table does not give an external reviewer authority to make that decision. The MD’s approval of the policy, breach plan and final pack remains separate from the DPO’s day-to-day accountability.

For requests and operational tasks, department heads should identify a named internal contact and a cover arrangement. The DPO should resolve any uncertainty about legal duties with a Singapore-qualified lawyer.

4. Open actions carried over from B2

The table below is copied from the B2 tracker on handover day, so the dates and owners match B2 exactly. The dates are proposed targets, not evidence that work has started or closed. After handover, B2 is the master copy; update it, not this table.

Gap ID	RAG	Action	Owner	Due	Evidence to close
G-01	Amber	Adopt the data protection policy, publish the DPO contact and document the complaints process; update B2.	Head of Operations, appointed DPO	30 Nov 2026	MD-approved policy, website capture showing dpo@quillmarrow.example, and documented complaints process.
G-02	Amber	Remove the pre-ticked marketing box, establish an affirmative consent record for showroom sign-ups and update B2.	Head of Marketing	13 Nov 2026	Updated B2B form, showroom sign-up process and sample consent records showing the person's choice and its source.
G-03	Amber	Document permitted CCTV purposes and access, prohibit unrelated use unless reviewed and authorised, and record the change in B2.	Showroom Supervisor	15 Dec 2026	Approved CCTV purpose and access procedure, staff communication record and documented approval route for exceptional use.
G-04	Red	Replace the website statement and prepare notices for job applicants, showroom sign-ups and CCTV; record the work in B2.	Head of Operations, appointed DPO	13 Nov 2026	Approved notices and dated screenshots or copies showing publication at each specified collection point.
G-05	Amber	Adopt the access and correction procedure, log the AR-01 to AR-06 scenarios and train receiving teams; update B2.	Head of Customer Service	13 Nov 2026	Approved procedure, request log template, completed scenario walkthroughs and staff briefing record.

Gap ID	RAG	Action	Owner	Due	Evidence to close
G-06	Green	Retain evidence of the Sales verification cycle and document how corrections are reflected in relevant records; update B2.	Sales Manager	29 Jan 2027	Dated verification record and documented correction procedure or sample completed correction record.
G-07	Amber	Review external-link settings and privileged access, enable MFA for ShopCloud admin where available, and record remediation in B2 and B11.	IT Manager	13 Nov 2026	Dated access review, ShopCloud admin MFA configuration evidence, SharePoint sharing-control evidence and remediation record linked to B11.
G-08	Red	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, appointed DPO	15 Dec 2026	Approved B8 schedule covering RS-01 to RS-20, with owners, disposal methods and documented accountant or lawyer confirmation where relevant.
G-09	Amber	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, appointed DPO	15 Dec 2026	Written ShopCloud hosting-region confirmation and documented DV-01 contract review with agreed transfer safeguards or recorded unresolved issues.
G-10	Red	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, appointed DPO	13 Nov 2026	MD-approved B11, completed tabletop exercise record using INC-2026-07 and logged corrective actions.
G-11	Amber	Document the campaign DNC check and suppression process, standardise sender details and record the check in B2 before calls begin.	Head of Marketing	13 Nov 2026	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).

Do not close a vendor or security action solely because a supplier has promised a change. Record the evidence received, the reviewer, the date and any remaining exception. If a target cannot be met, the owner should propose a revised date and interim handling for the DPO and COO to consider.

5. Live items on day one

These need attention in the first week, before the routine starts.

Item	Why it is live	Owner	Next step
AR-06 access or correction request via DV-01	Open in the B7 log; scope and identity not yet confirmed	Head of Operations, appointed DPO	Contact the requester directly, confirm scope and identity, and record the date Quillmarrow received it
INC-2026-07 follow-up actions	Assessed and recorded as not notifiable on 16 September; lessons logged but sharing controls not yet changed	IT Manager	Restrict "anyone with the link" sharing (G-07) and file the evidence in the B11 incident record
Planned telemarketing campaign	No DNC process yet; two of five list sources lack consent evidence	Head of Marketing	Hold the campaign until the B12 go or no-go gate is met
Enterprise customer questionnaire	Asked for the privacy policy, breach plan and retention schedule	COO	Answer only with documents the MD has approved (B5, B11, B8), and say which are still drafts

6. Maintenance calendar

The calendar is a proposed operating rhythm for **November 2026 to October 2027**. In every month, the DPO should review B2 actions, new incidents, requests, complaints and changes to data uses; check owners and due dates; and report material issues to the COO. Record “none” only after checking with the relevant owners.

Month	Additional planned tasks
November 2026	Confirm pack ownership and locations; publish the DPO contact; start B7 intake and the B2 action review; arrange the staff briefing.
December 2026	Seek B11 approval and test the incident reporting route; review notice, marketing and DNC actions; check access-control evidence with the IT Manager.
January 2027	Confirm B8 retention decisions and the CCTV setting; review DV-01 safeguards and DV-02 hosting evidence; report overdue actions to the MD and COO.
February 2027	Review B3 with department heads for new or changed data uses; check whether staff questions or requests reveal process gaps.
March 2027	Sample request handling and consent records; check that access is restricted and actions from the sample are assigned.
April 2027	Review vendor and transfer changes against B9 and B10; check outstanding contract, hosting and administrator-access evidence.
May 2027	Review retention clean-up progress, holds and vendor-held records, including **RS-20**; record any exceptions.
June 2027	Run a short B11 reporting exercise with relevant roles; update the contact list and track lessons.
July 2027	Review notices, forms and marketing practices with the relevant department heads; check the DPO contact remains visible.
August 2027	Review B3 and system-access changes with IT and department heads; check whether any new processing needs an impact assessment.
September 2027	Review training attendance and arrange follow-up for staff who missed the briefing; check B14 against the separate AI governance pack.
October 2027	Carry out the annual pack review; present an action and decision summary to the COO and MD and propose the next calendar.

Before any marketing campaign, use B12 rather than waiting for a calendar review. Before a material new data use, vendor arrangement or transfer, update the relevant inventory and assessment first.

7. First 90 days checklist

The periods below run from the proposed handover at the start of November 2026. They are working targets; the DPO should adjust dates with the COO and record changes in B2.

First 30 days

1. **Confirm the handover:** check the B1–B16 files, their owners, approval status and actual SharePoint locations. Separate drafts from approved documents.
2. **Make contact routes clear:** arrange website publication of **dpo@quillmarrow.example**, tell staff how to reach the DPO and test the mailbox.
3. **Start the action routine:** reconcile the table above with B2, confirm each owner and due date, and schedule a monthly review.
4. **Set up requests:** agree how Customer Service, HR and the Malaysia partner forward requests; establish the B7 log and identity-check process. Close out AR-06, which is still open.
5. **Brief the sponsor:** tell the COO which approvals, legal questions and immediate control decisions remain open.

By 60 days

1. **Put incident arrangements in place:** seek MD approval of B11, confirm contacts and run a short reporting exercise with the IT Manager and department heads.
2. **Review collection and marketing:** check notice and consent work under G-02 and G-04, and require B12 checks before the planned campaign.
3. **Check access and vendors:** review evidence for SharePoint sharing, DV-02 administrator MFA and DV-03 administrator access; record exceptions.
4. **Deliver the briefing:** use B15 once the instructions and contact routes are confirmed. Ask HR to retain attendance and follow up with absent staff.

By 90 days

1. **Decide retention actions:** obtain record-owner input for B8, verify the CCTV setting and agree a controlled clean-up plan that accounts for holds.
2. **Review overseas transfers:** confirm what is sent to DV-01, how often and by which channel; obtain evidence of safeguards and the DV-02 hosting region. These details remain unverified.
3. **Report to the MD and COO:** summarise completed actions, evidence, overdue items, decisions needed and proposed next dates. Keep open items open until evidence has been reviewed.

8. Publishing the DPO's business contact information

The DPO's intended business contact is **dpo@quillmarrow.example**. Its website publication is outstanding under **G-01**.

The DPO should ask the IT Manager to confirm that the mailbox receives messages, identify who monitors it and arrange cover for absences. Ask the website owner to publish the contact in an accessible location, including the website privacy notice, and check the relevant notices and collection points for a consistent contact route. The DPO should confirm the appropriate wording and placement with a Singapore-qualified lawyer.

After publication, keep a dated screenshot or link and test the contact route. Record the result in B2. Review the contact after a website change, mailbox change or change in responsibility; a draft notice or an instruction to publish is not evidence that the contact is live.

9. When to call for help

- **Singapore-qualified lawyer:** seek advice on legal interpretation, notice and consent wording, a difficult access request, proposed retention decisions, overseas transfer safeguards or breach notification questions. For accounting and tax retention needs, confirm the relevant periods with an accountant or lawyer.
- **Forensic specialist:** involve an appropriately qualified specialist where the facts, access history or containment needs cannot be established with available skills. Coordinate through the IT Manager and DPO, preserve available evidence and follow B11; do not disturb logs unnecessarily.
- **The reviewer:** if Quillmarrow separately agrees ongoing support, the DPO may ask the reviewer to review the action tracker, prepare for a management discussion or help organise a document update. The reviewer supports Quillmarrow's appointed DPO and does not replace the DPO, legal adviser or incident decision makers.

Escalate promptly when an issue is urgent. Do not wait for the next scheduled review to report a suspected incident or an overdue decision with material consequences.

10. Sign-off

Signing confirms acceptance or acknowledgement of the handover as described; it does not by itself approve every proposed control, close an action or establish implementation. Attach or reference any exceptions and outstanding decisions.

Role	Confirmation	Signature	Date
Head of Operations / DPO	I accept the day-to-day handover and the open actions recorded for follow-up.	_____	_____
Managing Director	I acknowledge the handover, the open actions and the decisions requiring management attention.	_____	_____

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).