PDPA PROGRAMME PACK · B8

Retention schedule

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	B8 · Retention schedule
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Head of Operations (DPO); MD confirms decisions
Label	Fictional organisation, illustrative only, not a client case study

1. How to read this schedule

The schedule sets out proposed decisions for Quillmarrow's records, not universal retention periods. Read each row with the personal data inventory in B3 and the actions in B2. The record owner should confirm where the information is held, including copies held by providers, before applying a decision.

The retention clock starts at the **trigger stated in the row**, not necessarily when the information was first collected. For example, a trigger may be an account becoming inactive or an employee leaving. The owner should check that the trigger can be identified from reliable records.

A row marked **Proposed** needs Managing Director (MD) confirmation before it is adopted. Where a period or trigger remains open, the owner should seek a decision rather than invent one. Legal retention drivers are flagged for confirmation with Quillmarrow's accountant or a Singapore-qualified lawyer, particularly for accounting and tax records. Do not treat a proposed period as a statement of law. Every number in this schedule is Quillmarrow's own business proposal for the MD to accept or change; none of them is a period set by law. Where a law may set a period, the row says so and leaves the number to the accountant or lawyer.

2. How the decisions were made

Each proposed decision starts with the purpose for which the information was collected or used. The owner should ask when that purpose ends, whether a continuing legal or business need remains, and what risk arises from keeping the information longer than necessary.

The review should consider disputes, outstanding requests, investigations and other documented reasons to preserve particular records. Apply a specific hold where needed and review it; a hold should not become a reason to retain every record indefinitely. Confirm legal questions with a Singapore-qualified lawyer.

G-08 records that Quillmarrow has no schedule and generally keeps information indefinitely. The reported CCTV overwrite setting of about 30 days is client-reported and still needs verification; it is not evidence that other records are disposed of.

3. Disposal and evidence

After the MD confirms the relevant decision, the record owner should identify eligible records, check for holds and authorise disposal. The IT Manager should coordinate system changes and any work by Fictional Harbour IT, DV-03. The DPO should review exceptions and unresolved questions.

Use the appropriate method for each location: delete eligible records from live cloud systems and shared files, arrange deletion with the relevant provider, and securely destroy paper records. For the CCTV recorder, confirm its overwrite setting and how saved exports are handled. For DV-01, agree and verify the disposal of Malaysia delivery records under RS-20; do not assume Quillmarrow can delete the partner's copies directly.

Keep a disposal record showing the record type, selection criteria, date, owner, method, systems or providers covered, and evidence or outstanding confirmation. Avoid placing the deleted personal data in the disposal log.

Backups may age out separately from live records. The IT Manager should confirm backup cycles and provider capabilities, document the expected removal route and prevent routine restoration from reintroducing disposed records. Where selective deletion is not possible, record the limitation and controls. Evidence of backup arrangements and provider deletion remains to be obtained.

4. Decisions needed from management

G-08 is Red in B2, with a target of **15 December 2026** for approved decisions. The DPO brings the rows to the MD in three groups so that the easy decisions are not held up by the hard ones:

Group	Rows	What the MD decides	Input needed first
Ready to approve	RS-01, RS-03, RS-04, RS-05, RS-06, RS-10, RS-11, RS-16, RS-18, RS-19	Accept or change the proposed period and trigger.	Owner confirms the system can find records by the trigger date.
Needs outside confirmation	RS-02, RS-13 (accountant or lawyer); RS-12, RS-14, RS-17, RS-20 (lawyer)	Approve once the confirmation is filed.	Finance Director or DPO obtains written confirmation.
Needs a factual check	RS-07, RS-08, RS-09, RS-15	Approve after the check.	Marketing confirms consent and DNC records (B6, B12); IT verifies the CCTV overwrite; HR completes the NRIC/FIN necessity review.

Evidence that G-08 can close: the MD-approved schedule (all 20 rows marked Approved or Open with a reason), named owners for each row, the first disposal records, and the verified CCTV setting. Until then, G-08 stays open in B2 and no bulk deletion starts (see the B2 interim measures).

5. First clean-up after approval

These follow the MD's decisions. Each one needs a hold check before anything is deleted.

First clean-up	Owner	Target date
Verify the CCTV overwrite setting and identify saved footage due for review under RS-09, PD-13.	Showroom Supervisor, with IT Manager	30 November 2026 (a check, not a deletion)
Identify unsuccessful applications beyond the approved RS-11 period; dispose of eligible CVs in PD-15.	HR Manager	15 January 2027
Review the need for staff NRIC or FIN copies, PD-19, and dispose of copies with no justified need under RS-15.	HR Manager	15 January 2027
Identify inactive web-shop accounts under RS-01 and review linked orders before disposing of eligible PD-01 records.	Head of Customer Service	31 January 2027
Review old helpdesk tickets and chat transcripts, PD-06, against the approved RS-05 decision.	Head of Customer Service	28 February 2027

The DPO reviews the schedule at least once a year and whenever B3 records a new system, vendor or collection point.

The 20-row retention schedule follows.

Schedule, part 1: decisions and triggers

ID	Record type	Inventory	Why keep it	Retention decision	Trigger	Status
RS-01	Web-shop customer accounts (inactive)	PD-01	Allow account reactivation or resolve account-related enquiries while the account remains useful.	Proposed: 24 months after the last account activity, then delete or anonymise unless a documented matter requires a hold.	Last customer account activity.	Proposed - to confirm with MD
RS-02	Orders, invoices and delivery records	PD-02, PD-03, PD-12, PD-23	Fulfil and support orders, reconcile payments, handle returns and disputes, and retain accounting and tax records as applicable.	Period set by law: confirm with your accountant or lawyer	Relevant accounting or tax record closure; confirm the appropriate trigger with your accountant or lawyer.	Open - legal input needed
RS-03	B2B account records (closed accounts)	PD-04	Resolve account queries and support orderly closure of business relationships.	Proposed: 24 months after account closure, excluding records that must be retained under RS-02 or a documented dispute hold.	B2B account closure.	Proposed - to confirm with MD
RS-04	B2B credit applications (declined)	PD-05	Document the application outcome and respond to related enquiries or disputes.	Proposed: 12 months after the decline decision, unless a documented dispute or other justified hold requires longer.	Date the applicant is informed of the decline.	Proposed - to confirm with MD
RS-05	Helpdesk tickets and chat transcripts	PD-06	Resolve service issues, respond to follow-up enquiries and identify related complaints.	Proposed: 24 months after ticket closure, unless linked to a continuing dispute or documented hold.	Ticket closure.	Proposed - to confirm with MD
RS-06	Call recordings	PD-07	Support the stated sales-line purpose and review a specific customer interaction where needed.	Proposed: 90 days after the call, unless a recording is needed for a documented complaint or dispute.	Date of the recorded call.	Proposed - to confirm with MD
RS-07	Marketing lists and consent records	PD-08, PD-09	Send marketing to people whose choices permit it and retain evidence of subscription, withdrawal or suppression.	Proposed: retain active subscription details while the subscription remains active; retain consent and suppression evidence for 24 months after withdrawal or list removal, subject to management and legal review.	Subscription withdrawal or removal from the active marketing list.	Open - legal input needed
RS-08	Telemarketing DNC check records	PD-10	Evidence that campaign numbers were checked and screened before calls were made.	Proposed: 24 months after the last call attempt for the campaign, subject to review of operational and legal needs.	Last call attempt for the relevant campaign.	Open - legal input needed
RS-09	Showroom CCTV	PD-13	Support the stated showroom security purpose and review relevant incidents.	Proposed: about 30 days after recording, consistent with the client-reported overwrite setting, unless footage is preserved for a documented incident; verify the setting.	Date and time of recording.	Proposed - to confirm with MD
RS-10	Visitor logs	PD-14	Support visitor access administration and follow up a site security matter if required.	Proposed: 6 months after the visit, unless a documented incident requires a hold.	Visitor's sign-out date or, if not recorded, the visit date.	Proposed - to confirm with MD
RS-11	Job applications (unsuccessful)	PD-15	Complete recruitment administration and respond to a query about the application outcome.	Proposed: 6 months after the applicant is informed of the outcome, unless a documented dispute or other justified hold applies.	Date the applicant is informed that their application was unsuccessful.	Proposed - to confirm with MD

ID	Record type	Inventory	Why keep it	Retention decision	Trigger	Status
RS-12	Employee HR files (after exit)	PD-16	Administer employment close-out and respond to relevant employment queries or disputes.	Open: MD to set the period after a Singapore-qualified lawyer confirms any legal driver for employment records. Separate payroll and CPF items (RS-13) and medical items (RS-14) first.	Employee's last day of employment.	Open - legal input needed
RS-13	Payroll and CPF records	PD-17	Administer payroll and CPF-related processes and retain accounting, tax and employment records as applicable.	Period set by law: confirm with your accountant or lawyer	Relevant payroll, CPF, accounting or tax record closure; confirm the appropriate trigger with your accountant or lawyer.	Open - legal input needed
RS-14	Medical certificates	PD-18	Administer employee leave and retain supporting records for the relevant employment process.	Open: MD to set the period after a lawyer confirms any legal driver for leave and medical records; keep only what is needed to administer leave.	Closure of the related leave record.	Open - legal input needed
RS-15	NRIC or FIN copies	PD-19	Purpose and necessity of retaining copies have not been established; review whether a copy is needed at all.	Open pending review of necessity; if no justified need is confirmed, securely dispose of existing copies.	Completion of the necessity review and any required identity-verification process.	Open - legal input needed
RS-16	Access and correction request log	PD-25	Track requests, response actions, decisions and completion of access or correction handling.	Proposed: 3 years after the request is closed, unless a documented complaint, dispute or legal hold applies.	Request closure.	Proposed - to confirm with MD
RS-17	Breach and incident records	PD-25	Document incident facts, assessment, notification decision, response actions and lessons.	Open: MD to set the period after legal review. Keep the incident record, assessment and decision log at least until all actions are closed and any regulator or legal matter has ended.	Incident closure after actions and review are recorded.	Open - legal input needed
RS-18	System audit logs	PD-21	Support security monitoring, incident investigation and review of access to systems.	Proposed: 12 months after log creation, subject to system capability, investigation needs and management review.	Log creation date.	Proposed - to confirm with MD
RS-19	Supplier contact records	PD-22	Manage supplier relationships and operational communications.	Proposed: 24 months after the supplier relationship ends, excluding transaction records retained under RS-02.	End of the supplier relationship.	Proposed - to confirm with MD
RS-20	Malaysia delivery records held by the partner	PD-11	Complete Malaysia fulfilment and delivery and resolve related delivery enquiries.	Proposed: 24 months after delivery completion, subject to review with a Singapore-qualified lawyer and alignment with any applicable RS-02 accounting or tax records.	Delivery completion.	Open - legal input needed

Schedule, part 2: owners, systems and disposal

ID	Owner role	System	Disposal method	Review	Evidence of disposal
RS-01	Head of Customer Service	Fictional ShopCloud	Delete or anonymise inactive accounts in Fictional ShopCloud; retain a dated deletion or anonymisation report for the IT Manager to verify.	Annual	Dated system report identifying disposed accounts, with the disposal action and any documented holds.
RS-02	Finance Director	Fictional LedgerOne, Fictional ShopCloud, Fictional PayGate and related files; confirm record locations.	After the confirmed period and any documented hold, delete or anonymise records in each system; obtain deletion evidence from relevant providers where needed.	Annual	Approved retention decision with accountant or lawyer confirmation where relevant, plus system disposal reports or provider confirmations.
RS-03	Sales Manager	Fictional StockPoint and Microsoft 365; confirm the system of record.	Delete or anonymise closed-account contact records in the system of record; retain a dated disposal report.	Annual	Closed-account disposal report recording the account reference, action date and any exception or hold.
RS-04	Finance Director	Fictional LedgerOne and related application files in Microsoft 365; confirm locations.	Securely delete electronic application files and confidentially destroy paper copies; retain a dated disposal record.	Annual	Dated deletion or confidential-destruction record linked to the application reference, without reproducing application contents.
RS-05	Head of Customer Service	Fictional Helpdesk	Delete or anonymise closed tickets and transcripts using the system's disposal function; retain a dated disposal report.	Annual	Dated system report showing the tickets deleted or anonymised and any records placed on hold.
RS-06	Sales Manager	Sales-line recording system; system and configuration not supplied.	Delete recordings through the recording system's retention controls; retain a dated disposal log.	Annual	System configuration record and dated deletion log; verify whether recording is enabled and how deletion is performed.
RS-07	Head of Marketing	Fictional MailBurst and showroom sign-up records; confirm storage locations.	Remove withdrawn contacts from active campaigns while retaining only the approved suppression evidence; securely destroy redundant paper sign-up records.	Annual	Dated MailBurst suppression and deletion report, disposal record for paper forms, and retained evidence of the person's marketing choice.
RS-08	Head of Marketing	Campaign record system; system not supplied.	Delete or securely destroy campaign check records at the end of the approved period; retain a dated disposal log.	Annual	Campaign DNC check and suppression records, followed by a dated deletion record. Checks must be made within the validity period set by the PDPC (confirm the current period).
RS-09	Showroom Supervisor	Showroom CCTV recorder (on site)	Allow verified automatic overwrite; document any export and secure deletion of incident footage when the hold ends.	Annual	Dated configuration check confirming overwrite settings, plus an incident-hold and deletion log where footage is exported.
RS-10	Warehouse Manager	Visitor log; format and storage system not supplied.	Securely destroy paper logs or delete electronic entries; retain a dated disposal record.	Annual	Dated destruction record or electronic deletion report showing the period covered.
RS-11	HR Manager	Recruitment files and Microsoft 365; system of record not supplied.	Securely delete electronic application files and confidentially destroy paper copies; retain a dated disposal record.	Annual	Dated deletion or confidential-destruction record linked to the recruitment case reference.
RS-12	HR Manager	Fictional PeopleDesk and Microsoft 365; confirm the systems of record.	Delete or securely destroy HR records at the end of the approved period, retaining records subject to a documented hold; obtain provider evidence where needed.	Annual	Approved retention decision and dated system deletion or destruction record, with documented exceptions and holds.
RS-13	Finance Director	Fictional PeopleDesk and Fictional LedgerOne; confirm systems and data flows.	After the confirmed period and any documented hold, securely delete or destroy records in each system; retain disposal evidence.	Annual	Accountant or lawyer confirmation where relevant, approved schedule and dated deletion or destruction reports.

ID	Owner role	System	Disposal method	Review	Evidence of disposal
RS-14	HR Manager	Fictional PeopleDesk and HR files; confirm the system of record.	Securely delete electronic certificates and confidentially destroy paper copies; retain a dated disposal record.	Annual	Dated deletion or destruction record, with access and hold exceptions documented.
RS-15	HR Manager	Onboarding files; storage system not supplied.	If retention is not justified, securely delete electronic copies and confidentially destroy paper copies; retain a disposal record without reproducing the identity details.	Trigger: necessity review	Documented necessity decision, lawyer confirmation where needed, and dated disposal record for copies no longer required.
RS-16	Head of Operations	Fictional Helpdesk or a controlled request log in Microsoft 365; system not yet established.	Delete or securely destroy closed request records at the end of the approved period; retain a dated disposal log.	Annual	Dated disposal report linked to request references, with any holds and exceptions recorded.
RS-17	Head of Operations	Microsoft 365 and controlled incident files; confirm the system of record.	Securely delete electronic records and destroy paper copies after the approved period; preserve any records on a documented hold.	Annual	Approved retention decision and dated deletion or destruction record, with incident reference and hold exceptions.
RS-18	IT Manager	Microsoft 365 and other relevant business systems; log sources not fully identified.	Apply verified system expiry or deletion settings; retain configuration evidence and a dated deletion or expiry report.	Annual	System-by-system retention configuration, dated access review and evidence of expiry or deletion.
RS-19	Finance Director	Fictional LedgerOne and Microsoft 365; confirm the system of record.	Delete or anonymise contact records in the system of record; retain a dated disposal report.	Annual	Dated deletion or anonymisation report linked to the supplier record, with transaction-record exceptions documented.
RS-20	Warehouse Manager	Records held by Tanjung Contoh Logistics Sdn. Bhd. (DV-01); partner system not supplied.	Request DV-01 to delete or anonymise records at the end of the approved period and provide written confirmation; retain the confirmation.	Annual	Agreed retention and deletion terms, dated written deletion or anonymisation confirmation from DV-01, and any documented hold.

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).