PDPA PROGRAMME PACK · B13

DPIA template, with a worked example

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	B13 · DPIA template, with a worked example
Version	1.0
Date	30 October 2026 (illustrative)
Prepared by	Alex Lew, reviewer and sign-off
Client approver (role)	Head of Operations (DPO)
Label	Fictional organisation, illustrative only, not a client case study

The PDPC recommends data protection impact assessments (DPIAs) as good practice; they are not a stand-alone statutory duty. This worked example follows the **PDPC Guide to Data Protection Impact Assessments**. It records proposed controls and an illustrative management decision, not evidence that the feature has been enabled or that the controls are operating. Legal questions should be confirmed with a Singapore-qualified lawyer.

1. Description of the change and why

Fictional PayGate offers a fraud-screening feature for Quillmarrow's web shop. The proposed feature would score orders using device data, IP address, delivery address and order history. An order identified for further attention could be held for review by Customer Service.

The proposed purpose is to help staff identify potentially fraudulent orders before fulfilment. Screening may reduce the need for staff to examine every order in the same way, but the case file provides no evidence of its effectiveness, accuracy or impact. Quillmarrow should not present those benefits as proven.

The change would introduce a new use of customer information and may create or extend the use of device and network data. A hold could delay a legitimate purchase or cause concern if a customer is unable to complete an order. The assessment therefore considers the information used, the vendor's role, customer notice, human review and the arrangements needed before launch.

The Head of Customer Service would own the operational process. The IT Manager would coordinate technical checks with Fictional PayGate and Fictional ShopCloud. The Head of Operations, Quillmarrow's appointed DPO, would advise on the assessment and open questions. The COO would decide whether the feature may proceed, subject to the conditions in section 7.

2. Personal data involved and data flow

The proposed flow below is a design for review, not a verified technical description. The IT Manager should obtain a field-level data flow and supporting vendor documents before launch.

1. A customer places an order through Fictional ShopCloud. Order and delivery information is associated with **PD-02**. Payment tokens and payment status are associated with **PD-03**; Quillmarrow does not see full card numbers through Fictional PayGate.
2. The proposed screening feature would use device data, IP address, delivery address and order history. Device and IP information should also be considered against **PD-24**, the website analytics and cookies inventory entry. The IT Manager and DPO should check whether B3 needs a new or amended entry to describe fraud-screening data accurately; its inclusion here does not establish that all such data is already collected for this purpose.
3. Fictional PayGate would return a score, flag or other screening result that may cause an order to be held. The exact score, fields returned, thresholds and systems that receive the result are not provided.

4. Customer Service would review held orders and record an outcome. It is not yet established where the result, staff notes or decision history would be stored, who could see them, or how long they would remain available.
5. Relevant order and review information may be retained or deleted in Quillmarrow's systems and at the vendor. Applicable periods and deletion arrangements are open decisions under B8.

The vendor's processing and hosting locations, any onward transfers and subcontractors, and any proposed reuse of data are **not provided**. Nor is there evidence of the security measures for the new feature. The DPO should review Fictional PayGate under B9 and, if an overseas transfer is identified, use B10 to assess the flow and proposed safeguards.

3. Necessity and proportionality

The stated aim is to identify orders that warrant a fraud review. Before approval to launch, Quillmarrow should ask whether the feature is needed for that aim and whether a less intrusive approach could achieve it. The case file does not establish the frequency or nature of fraud, the effectiveness of existing checks, or the feature's expected performance. The Head of Customer Service should document the operational problem and available alternatives rather than assume that more data will produce a better result.

The IT Manager should obtain a field list showing what is sent, collected, inferred and returned. For each field, the service owner should record why it is needed, whether it is mandatory and whether it can be reduced. In particular:

- Confirm what "device data" includes and whether persistent identifiers are used.
- Explain the role of the IP and delivery addresses and the scope of order history requested.
- Check whether the feature collects information before an order is submitted and whether it affects customers who do not complete checkout.
- Limit staff access to screening results and review notes to roles that need them.
- Set proposed retention and deletion arrangements for raw device data, scores and review records; obtain vendor confirmation and update B8.

Screening information should be used for the stated fraud-review purpose, not added to marketing audiences or used for another unrelated purpose without a separate assessment and appropriate authorisation. Quillmarrow should also test whether staff can understand and challenge a hold without needing unnecessary information about the customer.

4. Risks and controls

Likelihood and impact are illustrative judgements for the proposed design, not measured results. **Residual ratings are conditional** on the further controls being implemented and verified; until then, the risks remain open. The DPO should revisit the ratings when vendor evidence and testing are available.

Risk	Likelihood	Impact	Existing controls	Further controls	Residual (Low/ Medium/ High)	Owner
A legitimate customer's order is wrongly held, causing delay or missed delivery.	Medium	Medium	No feature-specific control evidenced.	Customer Service reviews holds within one working day; no automatic cancellation. Test with representative scenarios and monitor outcomes.	Medium	Head of Customer Service
Staff rely on a score without examining the order, leading to an unfair or unexplained outcome.	Medium	High	No review procedure evidenced.	Provide a review guide, record reasons and allow escalation. Staff must not treat a score alone as a final decision.	Medium	Head of Customer Service
Device or order data is reused for marketing or another purpose.	Medium	High	Purpose restriction for this feature not evidenced.	Restrict the stated purpose; check access, system configuration and vendor terms. Require separate review before any new use.	Medium	Head of Marketing

Risk	Likelihood	Impact	Existing controls	Further controls	Residual (Low/ Medium/ High)	Owner
Device data or screening results are retained longer than needed.	Medium	Medium	No feature-specific retention decision evidenced.	Agree periods and deletion triggers with the DPO; obtain vendor evidence and update B8.	Medium	IT Manager
Fictional PayGate reuses the data for its own purposes beyond Quillmarrow's instructions.	Medium	High	Feature-specific vendor terms not provided.	Review permitted use, subcontractors and evidence under B9; resolve proposed reuse with the vendor and a lawyer.	Medium	Head of Operations, as DPO
Data is stored, accessed or transferred outside Singapore without understood safeguards.	Medium	High	Processing locations and transfer arrangements not provided.	Map locations and onward transfers; assess proposed safeguards under B10 with a lawyer before launch.	Medium	Head of Operations, as DPO
Customers do not understand that screening occurs or that an order may be held.	Medium	Medium	Current notice is a generic website statement from 2019.	Update B4 notice A, place it appropriately at checkout and test that it is accessible before launch.	Low	Head of Marketing
Screening data or results are disclosed to unauthorised people.	Medium	High	Microsoft 365 MFA is reported, but the feature's systems and access controls are not established.	Confirm access restrictions, secure transmission, logging and vendor security evidence; test relevant access.	Medium	IT Manager

The ratings do not mean that the remaining risk is accepted. The COO should review any control that cannot be evidenced, any material uncertainty and the proposed response before launch. Track actions in B2, particularly under G-03, G-04, G-07, G-08 and G-09.

5. Human review

The proposed operating rule is that **Customer Service reviews held orders within one working day; there is no automatic cancellation**. This is a condition of the illustrative decision, not an established current practice. The Head of Customer Service should document cover for absences and the route for an unresolved or urgent order.

A reviewer should inspect the information needed to understand the hold, consider relevant order context and decide whether to release the order, seek proportionate clarification or escalate it. A hold should not be treated as proof of fraud. If a score or flag is the only information available, staff should escalate rather than invent a reason for the result.

The review record should identify the order reference, hold and review times, reviewer role, information considered, action taken and reason. It should avoid unnecessary device details or sensitive free-text notes. The customer should have a contact route for questions and, where appropriate, be told about a delay without disclosing information that would undermine a legitimate security check. Confirm the wording and any legal questions with the DPO and a lawyer.

The Head of Customer Service should periodically review held-order outcomes and delays, including complaints and cases where a hold was reversed. The IT Manager should investigate patterns that may indicate a configuration problem. Any changes to thresholds or automated actions require the review described in section 8.

6. Notice and consent impacts

The Head of Marketing should update **B4 notice A** to explain the proposed fraud-screening purpose in plain language, the relevant categories of information, the role of Fictional PayGate and the possibility that an order may be held for human review. The notice should include Quillmarrow's DPO contact, **dpo@quillmarrow.example**, and be made available at the appropriate point in checkout.

Before publication, the DPO should compare the wording with the verified data flow and vendor terms. The current case file does not establish the processing location, all recipients, the use of cookies or identifiers, or whether the vendor proposes its own use of the data. The notice must not imply those questions have been resolved.

The team should assess the appropriate basis and any consent implications for the actual feature, including any relevant device or cookie collection, with a Singapore-qualified lawyer. The existing checkout arrangement for order processing should not automatically be treated as resolving consent or notice questions for this new screening use. Record any consent wording and choices under B6 where applicable.

Customer questions, access or correction requests should follow B7 and be recorded against **PD-25**. Where a request concerns a screening result or information held by the vendor, the DPO should coordinate with Fictional PayGate rather than promise an outcome before checking the facts.

7. Illustrative decision: proceed with conditions

Decision maker: COO, with advice from the Head of Operations as DPO.
Illustrative decision: Proceed with preparation, and permit launch only when the conditions below are completed, evidenced and accepted. This worked decision does not establish that approval or launch occurred.

Condition before launch	Owner	Target date	Evidence for the COO and DPO
Document the purpose, alternatives and field-level data flow, including the score and hold mechanism.	IT Manager	13 November 2026	Reviewed data-flow diagram and field list; updated B3 entries for PD-02, PD-03 and PD-24 as appropriate
Complete the B9 vendor review, including security, permitted use, subcontractors and incident contacts. Resolve material contract questions with a lawyer.	Head of Operations, as DPO	30 November 2026	Vendor responses, supporting documents, legal advice and recorded open issues
Confirm processing locations and assess any overseas transfers and safeguards.	Head of Operations, as DPO	30 November 2026	Location evidence and B10 assessment, where applicable
Agree retention and deletion arrangements for device data, scores and review records.	IT Manager	30 November 2026	Approved decisions, vendor confirmation and B8 updates
Prepare and test the human-review process, including the one-working-day target and no automatic cancellation.	Head of Customer Service	11 December 2026	Procedure, test scenarios, results and escalation route
Update and review B4 notice A; resolve consent questions with a lawyer.	Head of Marketing	11 December 2026	Approved notice wording, checkout placement and advice record
Reassess risks and make the launch decision against the evidence.	COO	18 December 2026	Completed action record, DPO advice and dated decision with reasons

If a condition is unmet, the COO should hold launch and record the remaining action. The reviewer may support the assessment; Quillmarrow's appointed DPO and management retain their respective responsibilities.

8. Review triggers

The DPO should reopen this assessment before a material change to the screening data, purpose, vendor, subcontractors, processing location or retention arrangements. Review is also needed if Quillmarrow proposes automatic cancellation, changes the hold threshold, finds repeated wrongful holds, receives a relevant complaint or request, or identifies a security incident.

The Head of Customer Service and IT Manager should provide the DPO with operational findings and vendor changes. Record the revised risks, controls, owners and decision in B2 and update B3, B4, B8, B9 or B10 as needed. A review date and cadence should be agreed at launch; none is evidenced yet.

9. Blank template guidance

To reuse this structure, describe the proposed change and purpose, map the information and recipients, assess necessity and alternatives, and record risks to individuals and Quillmarrow with existing evidence and further controls. Assign owners and dates, document human review and notice or consent impacts, and record a management decision separately

from the assessment. Mark unknowns as missing, set review triggers and obtain appropriate legal advice; do not treat a completed template as proof that controls operate.

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).