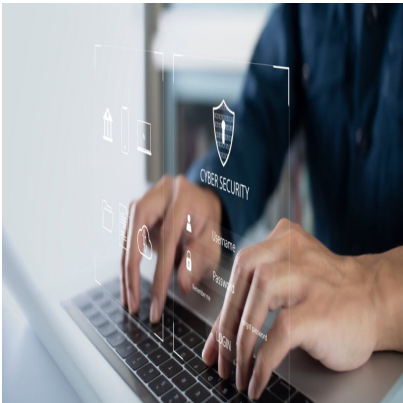




PDPA Access Request: Build the 30-Day Response File

Description

Acknowledge the request, verify the requester, define the data and use information sought, search relevant systems, assess applicable exceptions and respond within 30 calendar days or explain the valid next step.

Start one clock

Log receipt time, channel, requester and exact words. The review checklist uses 30 calendar days, not working days. Assign an owner and reviewer on day one. ([PDPC access review checklist](#))

An access request can concern personal data and information about how it was used or disclosed. Turn each requested item into a search row.

Situation	What changes
Request is broad or ambiguous	Clarify scope promptly without stopping internal preservation
Identity is uncertain	Verify proportionately before disclosing personal data
Third-party or excepted material appears	Review and redact only on a documented basis
Search will exceed the normal period	Send a reasoned update and preserve the full timeline

Related: [compare the distinct correction-request workflow](#)

Search by system owner

List email, CRM, support, payment, CCTV, HR and archive systems that may contain responsive data. Record the query, date range and custodian even when nothing is found. ([PDPC Key Concepts Guidelines](#))

Ask only for identification proportionate to the disclosure risk and deliver through an agreed secure channel. Do not send a sensitive export to an unverified address.

Example: If a request arrives on 3 August, count 30 calendar days from receipt using the organisation's documented method and set internal search and legal-review deadlines well before the final response date.

Document exceptions narrowly

Third-party data, legal restrictions and statutory exceptions require a reasoned review. Redact or withhold only the affected portion where possible.

Keep the acknowledgement, clarification, searches, decision, disclosed copy and delivery proof. A defensible no-record result still needs a reproducible search log.

- Log the exact request
- Verify identity
- Clarify scope
- Preserve relevant records
- Search every mapped system
- Review exceptions and redactions
- Deliver securely and retain proof

Related: [prepare separately for a notifiable breach](#)

Date Created

11/08/2026

Author

rachelng