

PDPA 2024 Compliance Checklist

A practical, 38-point audit for Malaysian organisations preparing for the Personal Data Protection Act 2024 Amendment.

38

audit points

6

key obligations

RM 1m

max penalty

Who this is for

Every organisation in Malaysia that collects, stores, processes, or disposes of personal data. That includes customer records, employee files, supplier contracts, patient records, financial statements, CCTV footage, and anything else that can identify a living individual.

What changed in 2024

The Personal Data Protection (Amendment) Act 2024 (Act A1709) introduced significant changes to Malaysia's PDPA regime, now in force. Penalties for unlawful processing or disclosure rose to a maximum fine of **RM 1 million** or **3 years' imprisonment**. New obligations include mandatory appointment of a Data Protection Officer for larger processors, explicit data breach notification requirements, and stricter rules around cross-border transfer.

How to use this checklist

Work through each section in order. For every point, tick one of three boxes: **Yes** (you have this in place and can prove it), **Partial** (some evidence exists but not formally documented), or **No** (gap to address). Your score at the end tells you where you stand.

A note on document destruction

Sections 4 (Retention) and 5 (Disposal) are where most Malaysian organisations fail audits. PDPA Principle 5 requires personal data to be destroyed when no longer needed for the original purpose — but simply dragging files to a bin or using office shredders rarely provides defensible evidence. A compliant programme needs a written retention schedule, secure destruction by a vendor who issues tamper-evident certificates, and a verifiable chain of custody. Grass Stories exists to make that part effortless.

Your score

32-38 yes — **Audit-ready**. You are in the top 10% of Malaysian SMEs. Maintain and review annually.

24-31 yes — **Exposed but improving**. Prioritise the gaps in sections 2, 4, and 5.

16-23 yes — **Material risk**. A breach or audit would hurt. Start with appointing a DPO.

0-15 yes — **Act now**. Even one enforcement notice from the JPDP could stop operations.

1

Governance & accountability

Do you have the authority and structures to comply?

- 1.1

A named Data Protection Officer (DPO) has been appointed in writing and their contact details are publicly available.

☐ Yes ☐ Partial ☐ No
- 1.2

The board or senior management has endorsed a written personal data protection policy.

☐ Yes ☐ Partial ☐ No
- 1.3

A data protection budget is allocated annually, separate from general IT spend.

☐ Yes ☐ Partial ☐ No
- 1.4

Staff roles with data protection responsibilities are listed in job descriptions.

☐ Yes ☐ Partial ☐ No
- 1.5

The policy is reviewed at least once every 24 months or after any major incident.

☐ Yes ☐ Partial ☐ No
- 1.6

The organisation is registered with the Jabatan Perlindungan Data Peribadi (JPDP) if required by the 11 prescribed classes.

☐ Yes ☐ Partial ☐ No

Section 1 score

Yes count: _____ out of 6

2

Collection & notice

Do data subjects know what is happening to their data?

2.1 A written PDPA notice is provided to every data subject before or at the point of collection, in both English and Bahasa Malaysia.

☐ Yes ☐ Partial ☐ No

2.2 The notice clearly states the purpose, third-party recipients, and the subject's rights of access and correction.

☐ Yes ☐ Partial ☐ No

2.3 Consent is obtained separately for each purpose; bundled or pre-ticked consent is not used.

☐ Yes ☐ Partial ☐ No

2.4 Sensitive personal data (health, religion, political opinion, criminal record) is only collected with explicit consent.

☐ Yes ☐ Partial ☐ No

2.5 Children's data is only collected with parental consent and there is an age verification step in place.

☐ Yes ☐ Partial ☐ No

2.6 Website forms, contracts, and physical forms all carry the PDPA notice.

☐ Yes ☐ Partial ☐ No

Section 2 score

Yes count: _____ out of 6

3

Security & access control

Is personal data protected from unauthorised access?

3.1 Access to personal data is restricted on a need-to-know basis, with role-based permissions reviewed quarterly.

☐ Yes ☐ Partial ☐ No

3.2 All staff who handle personal data complete annual PDPA awareness training with a signed attestation.

☐ Yes ☐ Partial ☐ No

3.3 Laptops, phones, and removable media containing personal data are encrypted.

☐ Yes ☐ Partial ☐ No

3.4 Physical records are stored in locked cabinets or access-controlled rooms with CCTV.

☐ Yes ☐ Partial ☐ No

3.5 Visitor and cleaner access to data-handling areas is logged and escorted.

☐ Yes ☐ Partial ☐ No

3.6 A data breach response plan exists, has been tested, and names individual responders.

☐ Yes ☐ Partial ☐ No

Section 3 score

Yes count: _____ out of 6

4

Retention & minimisation

Do you keep data only as long as you legitimately need it?

4.1 A written retention schedule lists every personal data category and its retention period with legal justification.

☐ Yes ☐ Partial ☐ No

4.2 Retention periods do not default to "forever"; each has a defensible rationale (contract, tax, regulatory).

☐ Yes ☐ Partial ☐ No

4.3 An annual data audit identifies records past retention and flags them for destruction.

☐ Yes ☐ Partial ☐ No

4.4 Inactive customer, employee, and supplier records are reviewed at least once per year.

☐ Yes ☐ Partial ☐ No

4.5 Email archives, backup tapes, and shared drives are included in the retention schedule.

☐ Yes ☐ Partial ☐ No

4.6 There is a process to halt retention automatically when a legal hold or subject access request is in progress.

☐ Yes ☐ Partial ☐ No

Section 4 score

Yes count: _____ out of 6

5

Destruction & disposal

Can you prove personal data was destroyed securely?

5.1 Physical documents containing personal data are destroyed by cross-cut shredding (DIN 66399 level P-4 or higher) or by a certified destruction vendor.

☐ Yes ☐ Partial ☐ No

5.2 Every destruction event produces a tamper-evident Certificate of Destruction with a unique serial number.

☐ Yes ☐ Partial ☐ No

5.3 Certificates of Destruction are stored alongside the retention schedule for at least 7 years.

☐ Yes ☐ Partial ☐ No

5.4 Hard drives, USB sticks, and backup media are physically destroyed or cryptographically erased before disposal (not just formatted).

☐ Yes ☐ Partial ☐ No

5.5 Destruction vendors are audited at least once every 24 months for compliance with their own written procedures.

☐ Yes ☐ Partial ☐ No

5.6 Chain of custody is maintained from collection point to final destruction, with witnessed sign-offs at each handover.

☐ Yes ☐ Partial ☐ No

5.7 Public tip-over bins, office shredders, and general waste are not used for personal data at any stage.

☐ Yes ☐ Partial ☐ No

Section 5 score

Yes count: _____ out of 7

6

Subject rights & breach

Can the organisation respond when things go wrong?

6.1 A documented process exists to respond to data subject access, correction, and deletion requests within 21 days.

☐ Yes ☐ Partial ☐ No

6.2 A data breach register records every suspected incident, regardless of whether it was notifiable.

☐ Yes ☐ Partial ☐ No

6.3 Breach notification procedures follow JPDP's Incident Response Guidelines (Bahagian VIII), including timing and content requirements.

☐ Yes ☐ Partial ☐ No

6.4 Contracts with all data processors (vendors, cloud services, payroll) contain explicit PDPA clauses and audit rights.

☐ Yes ☐ Partial ☐ No

6.5 Cross-border data transfers outside Malaysia are documented and comply with the 2024 Amendment's transfer provisions.

☐ Yes ☐ Partial ☐ No

6.6 The organisation has simulated at least one data breach scenario in the past 12 months.

☐ Yes ☐ Partial ☐ No

Section 6 score

Yes count: ____ out of 6

Where do you stand?

Add up your 'Yes' answers across all 6 sections.

SECTION 1

Governance & accountab...

___ / 6

SECTION 2

Collection & notice

___ / 6

SECTION 3

Security & access cont...

___ / 6

SECTION 4

Retention & minimisation

___ / 6

SECTION 5

Destruction & disposal

___ / 7

SECTION 6

Subject rights & breach

___ / 6

Total score

___ / 38

Compare to scoring bands on page 2.

What to do next

If you scored below 24

Prioritise a Data Protection Officer appointment this quarter, and start building a written retention schedule. We run a 2-hour gap-analysis workshop for Malaysian SMEs — no cost, no sales pitch.

If Section 5 is your weakest

Secure document destruction is one call away. We handle the logistics, issue tamper-evident Certificates of Destruction, and maintain the chain of custody so your audit trail is bulletproof.

If you want to benchmark

Ready to close the gaps?

Email kelvin@grassstories.com or call +60 85 xxx xxxx

grassstories.com