Data Protection in Malaysia: Your 2025 Survival Guide

How the updated PDPA transforms data privacy and why it matters to every business

Data is the new gold. In today's hyper-connected world, how you collect, use, and protect it isn't just a technical matter—it's a matter of trust.

In Malaysia, that trust is regulated by the **Personal Data Protection Act 2010 (PDPA)**. And as of **July 2024**, Parliament has passed sweeping reforms through the **Personal Data Protection (Amendment) Act 2024**. These changes roll out in phases and will affect every business—from the corner café with a customer loyalty list to multinational corporations managing thousands of client files.

No matter your size, if you touch personal data, this law touches you.

The Timeline: What's Changing and When

The new compliance journey comes in **three phases**:

- **1 January 2025**—Initial updates take effect
- **1 April 2025**—Intermediate measures introduced
- **1 June 2025**—The heavyweights: mandatory Data Protection Officers (DPOs) for qualifying organisations and stricter compliance obligations

Sensitive vs. Non-Sensitive Data: Know the Difference

Not all data is created equal. The law draws a sharp line between "sensitive" and "non-sensitive" personal data. Why? Because some data can harm people more deeply if misused.

🔴 **Sensitive Personal Data includes:**

- Health records (physical or mental)
- Religious beliefs
- Political opinions
- Criminal records or allegations
- Biometric data (fingerprints, facial recognition, DNA)
- Financial information (*for DPO appointment thresholds*)

🟢 **Non-Sensitive Personal Data includes:**

- IC numbers
- Bank account details
- Employment history
- Spouse or family details
- Passport-sized photographs
- Contact numbers
- Membership IDs
- Race (*unless tied to religion, e.g., Islam*)
- Sexual orientation (*unless treated as a health condition*)

Notes:

- **Financial information** is not automatically "sensitive"—unless it triggers DPO requirements.
- **School records** and **CCTV footage** are classified as non-sensitive under current rules.

Tip: *"If data can be weaponised against someone, treat it like dynamite."*

Before & After: The PDPA in One Snapshot

Area	Before (PDPA 2010)	After (PDPA Amendment Act 2024)	Why It Matters
Terminology	"Data user" (entity controlling data)	"Data controller" (global standard term)	Malaysia now speaks the same language as GDPR—easier for multinationals.

Area	Before (PDPA 2010)	After (PDPA Amendment Act 2024)	Why It Matters
Sensitive Data	Health, religion, political opinions, criminal records	Adds biometric data and certain financial data	More data types now require explicit consent.
Deceased Persons' Data	Ambiguous	Explicitly excluded	Confirms PDPA applies only to the living.
Breach Notification	None	Mandatory to Commissioner + affected individuals	Forces faster response to protect victims and limit damage.
Processor Liability	No direct duty	Data processors now share legal obligations with data controllers	Third parties can now be prosecuted—controllers must choose vendors carefully.
Cross-Border Transfers	Only to minister-approved countries	Allowed to countries with "substantially similar" laws	Easier for businesses with global operations to move data lawfully.
Data Protection Officer (DPO)	Not required	Mandatory if: >20,000 personal data subjects OR >10,000 sensitive data subjects OR regular/systematic monitoring	Forces organisations with high data volumes or sensitive data to have an in-house or outsourced compliance lead.
Data Portability	Not provided	Individuals can request their data in a portable, structured format	Consumers gain more control (though less relevant for HR).
Penalties	Fine up to RM300,000, jail up to 2 years	Fine up to RM1 million, jail up to 3 years	Significantly higher stakes for non-compliance.

1. What the PDPA Covers (and What It Doesn't)

The PDPA regulates **personal data** in **commercial transactions**. In simple terms:

- **Personal data** = information about a living, identifiable person.
- **Sensitive personal data** = health, biometrics, religion, politics, criminal records, financial data (for thresholds).

The law applies to companies, organisations, and even law firms operating in Malaysia, but **not** to:

- Federal and state governments
- Data processed fully outside Malaysia (unless later processed here)

If you're collecting names, IC numbers, or biometrics—the PDPA applies.

2. The 7 Core Principles (Your Compliance Compass)

Break one, and you risk **RM1m fines, 3 years' jail, or both.**

1. **General**—Don't process personal data without consent (especially explicit for sensitive data).
2. **Notice & Choice**—Give a clear, bilingual privacy notice stating what you collect, why, and how it's used.
3. **Disclosure**—No sharing for unrelated purposes without consent.
4. **Security**— Protect data from leaks, hacks, or misuse—whether physical or digital.
5. **Retention**—Keep data only as long as needed, then destroy it.
6. **Data Integrity**—Keep information accurate, complete, and updated.
7. **Access**—Allow people to see and correct their data.

3. Consent: The Heart of PDPA

Consent can be:

- **Explicit**: e.g., a signed form for health data
- **Implied**: e.g., submitting a CV for a job application
- **Sensitive data** always = explicit consent.

Processing without consent is allowed only for contracts, law compliance, or protecting someone's life.

Practical tip: *Get consent early. Embed PDPA clauses into contracts—it saves headaches later.*

4. The New Amendments You Can't Ignore (Effective 2025)

The PDPA amendments are no longer on the horizon—they're here. As of **1 June 2025**, the key changes are fully in force:

- **"Data user"** becomes **"data controller"** (matching global terminology)
- **Biometric data** is now sensitive personal data
- **Deceased persons' data** excluded from scope
- **Mandatory breach notifications** for incidents likely to cause harm
- **Shared responsibility**—Data processors now face direct obligations and penalties
- **Cross-border transfers** simplified if the destination country has similar laws
- **Mandatory DPOs** if you:
    - Handle >20,000 personal data subjects, or
    - Handle >10,000 sensitive data subjects, or
    - Engage in regular/systematic monitoring (e.g., online tracking)

Bottom line: *If your organisation hasn't already appointed a DPO, updated policies, or reviewed your vendors—you're already behind.*

5. Why Employers Should Pay Attention

Employers = data controllers. That means:

- Get consent at hiring.
- Issue bilingual privacy notices.
- Protect both paper files and digital systems.
- Let staff access/update their records.
- Delete old data when no longer needed.
- Vet contractors (e.g., payroll vendors).
- Appoint a DPO if you meet thresholds.

Tip: *"Handle employee data like you handle salaries—with strict safeguards."*

6. Penalties and Remedies

- **Fines**: up to RM1,000,000
- **Jail**: up to 3 years
- **Both**: for serious cases

Employees and customers can complain to the **Personal Data Protection Commissioner**. While PDPA doesn't allow private lawsuits, claims may still arise under negligence or privacy torts.

7. Practical Steps to Stay Compliant

1. Update your privacy notices.
2. Audit your data volumes—do you need a DPO?
3. Train staff in data handling.
4. Encrypt systems and tighten access controls.
5. Draft a breach response plan (the DPO will manage this).
6. Audit regularly against the 7 principles.

Key Takeaways

- **Consent is power**—Get it clear, early, and documented.
- **Compliance is cultural**—Train and involve your people, not just your IT.
- **Security is ongoing**—Treat data like cash: lock it, monitor it.
- **The law evolves**—Data protection isn't static; keep adapting.
- **Prevention beats cure**— Stopping a breach is cheaper than fixing one.

Resources

- **PDPA Website**: pdp.gov.my
- **DPO Registration**: dafta.pdp.gov.my
- **Guidelines**: Available on PDPA portal for compliance and best practices

Final Word

The PDPA reforms are not just about avoiding fines—they're about **earning trust in a fragile digital world**. Businesses that respect privacy will stand out. Those that don't? They'll stand trial.

👉 ***Act early. Plan clearly. Protect data like you protect your bottom line.***

About the Author

Hi! I'm Esther Tang, a business lawyer based in Sarawak and Kuala Lumpur. I help organisations—from SMEs to corporates—navigate Malaysia's evolving legal landscape with clarity and confidence. Whether it's managing cross-border transactions, or building data protection frameworks, my goal is simple: to cut through the legal jargon and give business owners practical strategies they can actually use.

Get in Touch

The PDPA amendments are here. Is your business ready?

Whether you need a quick review of your data practices, guidance on appointing a Data Protection Officer, or a full compliance roadmap, we're here to help.

Let's future-proof your business together—so you can focus on growth while we take care of compliance.

📩 **Email:** esther@etsylaw.com

🌐 **Website:** www.etsylaw.com

📍 **Offices in Sarawak & Kuala Lumpur**