PDLEGAL

CTRL+ALT+COMPLY

RESPONDING TO DATA BREACHES THE PDPA WAY

May 2025

A. The System's Down - Is Your Data Gone Too?

When your system throws a 404 error, it usually just means a broken link. But if what's "missing" is your customers' personal data, you've got more than a tech glitch — you've got a compliance crisis. Under the Personal Data Protection Act 2012 (PDPA), any unauthorised access, disclosure, modification, or loss of personal data is considered a breach.

Whether it's a ransomware attack or a rogue employee clicking "Reply All" with an attachment they shouldn't have, understanding the nature of the breach is your first step toward a legally sound and reputation-saving response.

B. The CARE Framework: Don't Panic, Just Reboot Your Response

To manage a data breach in line with PDPA expectations, the Singapore Personal Data Protection Commission (PDPC) recommends the **C.A.R.E.** framework — four essential activities that guide a structured and effective response:

1. **Contain** the Breach

2. **Assess** the Risks and Impact

3. **Report** the Incident

4. **Evaluate** the Response and Prevent Future Breaches

C. Alt-Tab: Quickly Identifying and Containing the Breach (C)

As outlined in **Section 26B of the PDPA**, it is essential to act swiftly to prevent further exposure. This means:

1. Isolating affected systems;

2. Locking down data access; and

3. Starting a breach log immediately.

While immediate resolution may not be feasible, prompt action to contain a breach significantly improves the likelihood of mitigating damage and demonstrating regulatory compliance.

D. Press Ctrl: Time to Assess the Impact (A)

Once the situation has been stabilised, the next step is to assess the scope and severity of the breach. Key questions to consider include:

1. What types of personal data were involved?

2. How many individuals were affected?

3. What potential harm could result — for example, identity theft, financial loss, reputational damage, or other adverse consequences?

This assessment is critical for determining whether the incident qualifies as a notifiable data breach under **Section 26C of the PDPA**, organisations to evaluate and respond to data breaches in a "reasonable and expeditious manner."

E. To Report or Not to Report?

Not every data breach triggers mandatory notification requirements, although many do. Under **Section 26D of the PDPA**, read with Regulations 3 and 4 of the Personal Data Protection (Notification of Data Breaches) Regulations 2021, organisations are required to notify the PDPC within three calendar days of determining that a breach is notifiable.

A data breach is considered notifiable if it:

1. Is likely to cause significant harm to individuals, or

2. Involves 500 or more individuals.

Regulation 3 along with the Schedule to the Personal Data Protection (Notification of Data Breaches) Regulations 2021 provides guidance on what constitutes "significant harm." Examples include the unauthorised disclosure of NRIC numbers, medical records, financial account details, and other forms of sensitive personal data — essentially, any information that could result in real-world harm or distress.

F. Hit "Send": Making the Official Report to the PDPC

If the breach is reportable, notification to the PDPC must include the following details:

1. A clear account of the incident, including how it occurred and what systems or processes were affected.

2. Types of data affected.

3. Remedial actions taken to contain and resolve the breach.

4. Measures being implemented to prevent recurrence.

Section 26D(5) allows you to skip formal notification to the affected individuals if the breach is unlikely to cause significant harm e.g. if the data was encrypted or deleted remotely. However, even where notification is not legally required, providing a voluntary update to affected individuals can help maintain trust, demonstrate accountability, and manage reputational risk.

It is also important to note that **Section 26D(6) of the PDPA** provides that an organisation is prohibited from notifying any affected individual if law enforcement agency/ PDPC so directs.

G. No "Undo" Button: Evaluate and Prevent Future Breaches (E)

Once the immediate incident has been contained, it is critical to conduct a thorough review to identify root causes and strengthen future safeguards.

Key areas for evaluation include:

1. Root Cause Analysis: What systemic or procedural failures contributed to the breach?

2. Data Handling Practices: Were there lapses in how data was stored, transmitted, or accessed (e.g., improper use of cloud platforms)?

3. Security Infrastructure: Were existing measures—such as firewalls and access controls—adequate and properly configured?

4. Training and Awareness: Is additional staff training required, particularly in relation to data protection protocols and password hygiene?

Under **Section 12 of the PDPA**, organisations have a statutory duty to implement reasonable security arrangements to protect personal data. In practice, this requires moving beyond minimal compliance to establish a robust, proactive data protection framework that can effectively prevent future incidents.

H. Consequences: Not Just a Slap on the Wrist

Under **Section 48J of the PDPA**, the PDPC Is empowered to impose financial penalties of up to **S$1 million or 10% of annual turnover**, whichever is higher.).

However, the reputational damage from a data breach maybe more severe than a financial penalty. Clients don't forget breaches — especially the ones that make headlines. Transparency, speed, and good documentation are your best defence (next to not breaching at all).

And if you need motivation, consider these real-world examples:

1. One organisation was fined **S$50,000** for exposing personal data online with weak safeguards.

2. Another organisation was fined **S$30,000** for failing to secure and decommission an old portal.

3. The one that got away: one organisation got off with a **warning**, but only because of prompt action following a ransomware attack.

I. Prevention is Better Than Cure: Strengthen Your Defences Before It's Too Late

Implementing robust safeguards — like encryption, access controls, and regular audits can significantly lower your risk for a data breach.

We help organisations:

1. Evaluate their data protection practices.

2. Identify compliance gaps under the PDPA and PDPC guidelines.

3. Strengthen policies and breach response protocols.

In today's threat landscape, breaches aren't a matter of *if*, but *when*. The difference between a headline-grabbing fiasco and a well-handled incident lies in preparation, speed, and clarity of action.

Further information

Should you have any questions on how this article may affect you or your business, please get in touch with the following people:

T Dinesh
Counsel
tdinesh@pdlegal.com.sg

This article is intended to provide general information only and does not constitute legal advice. It should not be used as a substitute for professional legal consultation. We recommend seeking legal advice before making any decisions based on the information available in this article. PDLegal fully disclaims responsibility for any loss or damage which may result from relying on this article.