You Cannot Report a Data Breach You Cannot See

By: Jaiz Anuar

19 September 2025 · Data Governance · Privacy · 8 min read

Data breach notification begins with visibility: data inventory, meaningful monitoring, clear ownership and tested response readiness.

In 2025, data breach notification became a more immediate operational responsibility for organisations in Malaysia. This created an important question: how can an organisation report a data breach if it cannot see that the breach has happened?

A notification procedure, template and Data Protection Officer are important. But none will be effective if the organisation cannot detect the incident, identify affected data or determine who may have been impacted.

Data breach notification does not begin with a notification form. It begins with visibility.

A breach may exist before anyone recognises it

Not every breach creates an obvious security alert. Personal data may be downloaded using a legitimate account, a supplier may access information beyond scope, an employee may send records to the wrong recipient, or an API may expose customer information without triggering a traditional control.

The system may continue operating normally. There may be no ransomware, disruption or visible attacker activity. The organisation may remain unaware that personal data has been compromised.

The first challenge is not reporting quickly. It is knowing quickly.

You cannot assess data you do not understand

Once suspicious activity is detected, the organisation must determine what information was involved: whether personal data was exposed, its sensitivity, how many people were affected, whether it was protected, and whether it could enable fraud or identity theft.

A data inventory should identify what personal data is collected, where it is stored, which systems process it, who can access it, which third parties receive it, how long it is retained and what controls protect it.

A data inventory is not merely a compliance record. It is incident-response infrastructure.

Logging does not automatically create visibility

Many organisations collect large volumes of logs, but having logs does not mean a breach can be detected. Relevant systems may not be monitored, application logs may not record access to sensitive

data, supplier activity may not be visible, or retention may be too short to investigate.

Effective visibility connects identity, system activity and data context. Who accessed information? What data was accessed? Was it expected for that role? Was an unusual volume downloaded? Did access occur from an unfamiliar device or location? Was information transferred outside an approved environment?

The DPO cannot do this alone

Appointing a Data Protection Officer is important, but it does not transfer all responsibility to one person. The DPO depends on technology teams, cybersecurity investigators, data owners, legal and compliance teams, and management for evidence and decisions.

If these teams meet for the first time during a breach, valuable time will be lost. The process must be defined and exercised before an incident occurs.

Notification readiness must be tested

A written breach-response procedure may look complete until it is tested. Simulations expose practical gaps: can the organisation identify affected data, retrieve logs, contact owners, determine third-party involvement, make a notification decision within the required timeframe and explain the incident without unsupported assumptions?

Testing shows whether the organisation has the visibility, coordination and decision-making capability required during a real incident.

Reporting begins before the breach

Data breach notification is often treated as a legal activity after an incident. In reality, capability must be built earlier: when data is identified and classified, systems record meaningful activity and monitoring connects technical events with data risk.

An organisation cannot report what it cannot detect. It cannot assess data it does not understand. And it cannot respond quickly if ownership has never been established.

The notification form may be completed after the breach. The ability to complete it must be designed long before the breach occurs.

Question assumptions. Share knowledge. Build trust.