



TAX, STRUCTURE & COMPLIANCE

Notifiable Data Breach: There Are Two Clocks, Not One

30 days is for assessing eligibility. Notification itself carries no second buffer once eligibility is confirmed

A common and consequential misreading of Australia's data breach notification law is believing there is a single thirty-day window to handle the entire response. There are two separate clocks, and the second one, the notification itself, does not carry anything like the same buffer the first one does.

Which rules apply to your association?

The law depends on how your association is set up. A **company limited by guarantee** follows the Corporations Act 2001 (Cth) and its constitution. An **incorporated association** follows its state or territory associations Act and its rules. A **registered charity** also follows the ACNC Act and the ACNC Governance Standards, and some Corporations Act rules are replaced for charities that are companies. Check your own governing documents, and get advice before decisions with legal consequences.

In this resource

1. [The Two-Clock Structure Most Organisations Misunderstand](#)
2. [The Practical Escape Valve Worth Knowing Precisely](#)
3. [Why Documentation Matters As Much As The Decision Itself](#)

The Two-Clock Structure Most Organisations Misunderstand

Under the Notifiable Data Breaches scheme in the Privacy Act, an organisation that suspects a breach may have occurred, but does not yet know whether it qualifies as an eligible data breach, has up to thirty calendar days to conduct a reasonable and expeditious assessment to find out. The regulator treats this thirty days as a maximum, not a default timeframe to use in full, and expects organisations to move considerably faster wherever practically possible, since the risk of serious harm typically increases the longer a breach goes unaddressed. Agree in advance who decides whether to notify, and map other notifications, such as insurers, funders and other regulators, which may have shorter deadlines. As soon as there are reasonable grounds to believe an eligible data breach has occurred, which can be before a formal assessment ends, an entirely separate duty applies: the organisation must prepare a statement for the OAIC and notify affected individuals as soon as practicable, with no second thirty-day window attached to it at all. An organisation that spends the full thirty days on assessment, then assumes it has another thirty days to actually notify, has fundamentally misunderstood the scheme. The notification duty begins once there are reasonable grounds to believe the breach is eligible, and the expectation from that point is prompt action, not a second extended deadline.

The Practical Escape Valve Worth Knowing Precisely

A specific, practical provision rewards fast incident response. If an organisation takes remedial action before any serious harm to individuals actually occurs, action sufficiently effective that serious harm is no longer likely as a result, the notification obligation may not apply at all. This creates a tangible incentive to treat the early hours after discovering a suspected breach as the period where containment and remedial action can meaningfully change the organisation's legal position, not merely the practical severity of the incident.

Why Documentation Matters As Much As The Decision Itself

The assessment of whether a breach is likely to result in serious harm, and any decision that remedial action has removed that likelihood, needs to be documented as it happens. The regulator can request an organisation's reasoning, and a decision not to notify made without a clear, contemporaneous record of why is considerably harder to defend after the fact than one supported by documented, real-time reasoning.

- Understand precisely that the thirty-day period applies to assessing eligibility, not to the entire response, since notification itself must happen as soon as practicable once eligibility is established.
- Treat the immediate hours after discovering a suspected breach as the window for remedial action that may avoid the notification obligation entirely, not simply as containment for its own sake.
- Document the serious harm assessment and any remediation reasoning contemporaneously, since this record is what actually protects a decision not to notify if the regulator later asks for the reasoning.
- Confirm whether your association is covered, connecting directly to the privacy threshold discussion earlier in this series. Associations with annual turnover of \$3 million or less are often exempt, unless an exception applies, such as providing a health service or holding tax file number information.
- Build incident response capability into your cyber security planning discussed earlier in this series, since the speed of the organisation's response in the first hours directly affects its legal position under this scheme.

The Notifiable Data Breaches scheme rewards speed and honest documentation in roughly equal measure. An association that treats the thirty-day assessment period as an invitation to wait, rather than a maximum to beat, has misunderstood both the law and the practical incentive structure actually built into it.

This is one of the practical governance topics built into our Board Director course, alongside the papers, tools and frameworks that turn the principle into your board's actual practice. [Explore the course](#)

Annie Gibbins

Founder and CEO, Nexus Leadership

BOARDROOM ACTION WORKSHEET

Notifiable Data Breach: There Are Two Clocks, Not One

Turn the resource into evidence, a decision and an accountable next step. Keep the completed record in your association's approved board records system.

1 What is the issue or decision?

State the governance question in one clear sentence.

2 What evidence do we already have?

Record the facts, source documents and stakeholder evidence available now.

3 What evidence is still needed?

Identify the legal, regulatory, financial, member or operational information still required.

4 What is the agreed next action?

Capture the owner, timeframe and how the matter will return to the board.

Action owner	Review date	Board decision or resolution

General education, not legal, financial, tax, clinical or governance advice. Confirm specifics at the relevant primary source or with your own qualified adviser. Nexus Leadership is operated by Lipstick Consulting Pty Ltd · ABN 15 619 120 482.

CONTINUE YOUR LEARNING

Turn governance principles into practical board action.

Self-paced courses, editable resources and practical support for association boards and CEOs at nexusleadership.com.au.