



MEMBERSHIP, GROWTH & DIGITAL TRANSFORMATION

Data Governance Beyond Cyber Security: The Exposure Even Exempt Associations Have

Since June 2025, a statutory privacy tort has applied regardless of your turnover or exemption status

Many smaller associations, correctly, understand they currently sit below the \$3 million turnover threshold this series has already identified as the general Privacy Act compliance line. What fewer boards understand is that this threshold has real exceptions already in force today, and a separate, already-legislated legal exposure that applies regardless of turnover at all.

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 Exemption Still Stands, But It Is Narrower Than Most Boards Assume](#)
2. [The Separate Exposure Every Association Already Faces](#)
3. [What This Means For A Board Right Now](#)

The Exemption Still Stands, But It Is Narrower Than Most Boards Assume

The general small business exemption, based on the \$3 million annual turnover threshold discussed earlier in this series, remains in place as current law as at October 2026, with no confirmed date set for its broader removal despite the government having agreed in principle to eventually abolish it entirely. Reform is clearly the direction of travel, but boards should plan for it as a direction, not a deadline, given the ongoing uncertainty about timing and scope. What matters right now is that the exemption already carries real, current exceptions regardless of turnover. Organisations that provide a health service, trade in personal information, hold Commonwealth contracts, or are employer or employee associations registered or recognised under the Fair Work (Registered Organisations) Act 2009 are covered regardless of turnover, among other exceptions listed by the OAIC. An association that itself provides a health service, for example clinical services, assessments or health programs, even a small one, should confirm whether this specific carve-out already applies to it, rather than assuming the general turnover exemption automatically covers every organisation below the threshold.

The Separate Exposure Every Association Already Faces

Independent of the small business exemption entirely, a statutory tort for serious invasions of privacy has applied in Australia since 10 June 2025. It lets individuals sue any person or organisation, regardless of size, that intentionally or recklessly intrudes on their seclusion or misuses their information in a serious way. It is not a general right to sue over an accidental data breach, since negligence is not enough. This is a meaningfully different exposure from the general Privacy Act compliance regime this series discussed earlier. A currently exempt small association cannot rely on that exemption to protect it from this specific action, since the statutory tort operates on its own footing, aimed directly at serious privacy harms rather than routine compliance obligations. Being below the \$3 million turnover threshold protects

an association from the general Australian Privacy Principles compliance regime. It does not protect the association, or any individual who intentionally or recklessly misuses personal information, from a claim under the statutory tort, which sits on entirely separate legal footing.

What This Means For A Board Right Now

For organisations that are already covered, whether through the health information carve-out, turnover above the threshold, or another applicable exception, the penalties for serious or repeated non-compliance are severe: up to fifty million dollars, three times the benefit obtained from the breach, or thirty percent of adjusted turnover, whichever is highest. For organisations that remain exempt today, the clear direction of travel makes voluntary early preparation a sensible governance choice rather than a compliance obligation, particularly given how quickly the specific carve-outs already in force can catch an organisation that assumed the general exemption fully applied to it. Practical first steps are to confirm whether any exception applies, adopt a privacy policy and a data breach response plan, and check whether funder or government contracts already impose privacy obligations.

- Confirm precisely whether your association falls within an existing exception to the small business exemption, particularly the health information carve-out, rather than assuming the general turnover threshold automatically applies.
- Understand that the statutory tort for serious invasions of privacy applies regardless of your association's size or exemption status where privacy is invaded intentionally or recklessly, and build data-handling discipline around member and staff information accordingly.
- Build a simple data inventory now, mapping what personal information your association holds, where it is stored, and who has access, regardless of current exemption status, given the clear direction of privacy reform.
- Monitor the Tranche 2 reforms. An exposure draft bill was released for consultation in 2026 and is not yet law, and as at October 2026 it does not appear to remove the small business exemption. Do not assume today's exemption position is permanent, but avoid over-investing in compliance for requirements that have not yet been legislated.
- Connect this analysis directly to the cyber security discipline discussed earlier in this series, since data governance and cyber security are related but distinct obligations, addressing different risks even where the same underlying information is involved.

Privacy compliance in Australia is shifting, but it has not simply moved from exempt to covered overnight for every organisation. It has become a landscape of exceptions, a separate statutory tort that does not depend on turnover, and a clear reform direction worth preparing for early. A board that only checks the headline turnover threshold is checking half the picture. This is one of the practical governance topics built into our Association CEO 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

Data Governance Beyond Cyber Security: The Exposure Even Exempt Associations Have

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.