Getting ready for Privacy Act 2020

Simply Privacy

The Privacy Act 2020 comes into effect on 1 December 2020, giving organisations only a short window to take the steps necessary to be ready. Some organisations will have more to do than others, and some overseas organisations will be brought within the scope of NZ's Privacy Act for the very first time.

We've made a checklist of the things we think every one of these organisations should do before then. As always, we suggest taking a risk-based approach, prioritising the actions that impact on the more sensitive and/or high volumes of personal information that your organisation handles.

Get your governance settings right

- **Appoint** a Privacy Officer, if you haven't already – it's a mandatory requirement
- **Formalise** your privacy accountabilities and reporting, to ensure that privacy gets the appropriate level of attention and resourcing for your organisation's risk
- **Map** where personal information sits within your organisation's systems

Prepare for mandatory privacy breach notification

- **Ensure** the systems holding your more sensitive personal information enable you to determine who has accessed what and when in the event of a breach
- **Ensure** your service providers have satisfactory security safeguards in place
- **Ensure** your service providers are required to notify you of a privacy breach and help you deal with it
- **Ensure** your staff can identify a privacy breach and know who to report it to
- **Establish** a privacy breach response plan
- **Practice** your privacy breach response plan with the right people involved
- **Draft** some notification communications to have ready to go (for the Privacy Commissioner and affected individuals)
- **Think** about who else you might have to notify in the event of a privacy breach (e.g. insurers/NZX/Police)
- **Ensure** you can manage a privacy breach in the midst of a privacy breach (e.g. if you can't access your systems)

Consider the relevance of tweaks to other IPPs

- **IPP1 – Purpose of collection - Review** what personal information your organisation is collecting, including personal identifiers, and make sure it's all necessary
- **IPP4 – Manner of collection - Check** if you collect personal information directly from children/young people and if so, assess whether this is being done fairly, transparently and proportionately
- **IPP13 – Unique Identifiers - Ensure** you're taking appropriate steps to minimise the harm of misuse of your unique identifiers

Get ready for cross-border information sharing

- **Identify** what personal information your organisation is sharing overseas, and for what purpose
- **Remember** – disclosures to overseas service providers are not covered by the new IPP 12, but must comply with IPP 5 (your data must be protected from harm)
- If you're sharing personal information with a foreign entity that is not solely delivering services to your organisation, **ensure**:
    - An exception to IPP 12 applies to permit the disclosure (document your justification)
    - If you want to rely on the contractual exception, your current contracts provide for sufficient safeguards and limitations
    - Ongoing governance around cross-border information sharing, to ensure exceptions still apply (e.g. if relying on equivalent laws)

Fine-tune your processes for handling information requests

- **Check** your identification verification processes to see if they are fit for purpose, including:
    - how to reduce the risk of impersonation
    - whether your staff understand and can identify when an information request may be made under threat of physical or mental harm
- **Ensure** your information request process allows requests for urgency to be appropriately considered
- **Ensure** your automated deletion processes can be paused to allow for the retention of personal information that has been requested under IPP 6

Take the opportunity to improve general privacy hygiene

- **Check** your external facing privacy statement is accurate and easy to understand
- **Use** the new law as a lever to get your people thinking about privacy not just as a compliance exercise but as an opportunity to build trust
- **Consider** whether you need to review your insurance coverage
- **Consider** refreshing your information security awareness training for your staff – especially around email use and phishing, a significant cause of privacy breaches
- Don't forget your **employee** personal information – you have the same obligations there

---

Simply Privacy (www.simplyprivacy.co.nz) is a specialist consultancy providing privacy advice, strategy and consultancy services to public and private sector organisations. We believe in a holistic approach to privacy practice and we work with our clients to ensure that privacy solutions fit with their business needs and wider goals.

Please note that the contents of this checklist are not legal advice, and should not be taken as such.