Lynch & Co.
Corporate and Commercial Law
www.lynchandco.co.nz

Privacy Act 2020: What you need to know

By Sean Lynch, October 2020

The new Privacy Act 2020 will come into force on 1 December 2020. It will replace the Privacy Act 1993.

The new Act is likely only the start of a series of legislative reforms designed to keep New Zealand's privacy laws in line with international best practice.

Some key changes under the new Act are the introduction of:

- **a mandatory privacy breach reporting regime**: Any privacy breach which causes, or is likely to cause, serious harm will now need to be reported to both the Office of the Privacy Commissioner and to the affected individuals (unless an exception applies). Some key related points to note are:
    - "privacy breach" is defined very broadly and would include any unauthorised access or even denial of access to personal information, and objective criteria will be used to assess seriousness;
    - Even though the fine cap is relatively low at this stage ($10,000), the Privacy Commissioner has the power to publically disclose the breaching entity if there is sufficient "public interest" to warrant that, and so business reputational damage could be significantly higher than any fine; and
    - A quick and highly considered action plan will need to be progressed for any breach, and this is likely to be different for each type of breach.
- **restrictions on the transfer of personal information overseas**: There are now tighter restrictions and requirements applying to the transfer or personal information out of New Zealand. Clear criteria must be fulfilled in each case. For example, some 'permitted transfer' examples are where:
    - the foreign recipient is acting solely as the organisation's agent (for example, as a cloud storage provider), or
    - the information will continue to be protected by security safeguards comparable to those required by New Zealand law, or
    - the individuals concerned have given their consent after being told that their personal information may not be subject to the same protections as under New Zealand law.

- **Other**:
    - There is stronger emphasis on a primary recipient organisation remaining liable even though a secondary processor engaged by them is in default, e.g. a cloud services provider. Organisations therefore need to carefully assess the contract terms and other arrangements they have with such third parties.
    - The new Act increases the enforcement and compliance powers of the Privacy Commissioner, providing further tools to enable a more proactive role, including by issuing compliance notices and access directions, and by creating a range of new offences, punishable with fines of up to $10,000 (as noted above).

What Businesses and other Organisations Need to Do

We recommend all businesses and organisations collecting or holding personal information data to promptly do the following if they have not done so already:

- **Data Map**: Construct an accurate flow-chart, map or other diagram clearly depicting what types of personal information are collected; how and where received and stored (i.e. servers, systems and related security); where transferred to (if transferred); what countries / jurisdictions are involved; how long the information is stored for (and other privacy principles assessment); and what access restrictions and other data security measures apply, e.g. encryption.
- **Assess all Applicable Law**: Assess the applicable data protection law for each applicable country / jurisdiction. Assess all compliance issues under such law.
- **Consider / Review**:
    - all related contracting and other arrangements with third party suppliers;
    - your customer contracts, privacy statement, privacy policies and procedures, and staff training procedures – so they operate more effectively under the new Act;
    - all privacy-related governance documents (up to Board-level visibility);
    - relevant insurance policies; and
    - all privacy systems quality-review programmes to ensure they are up-to-date and active on a regular basis.
- **Make Changes**: Make changes to the above where required, and identify weak or risky areas that need improving.
- **Ensure you have a Privacy Breach Response Plan**: This will need to be flexible and scalable and will need to include key personnel including your key stakeholders; IT; legal; communications, and likely others as well.

If you require any legal assistance, please contact Sean Lynch at sean@lynchandco.co.nz, or ph 09 948 8433. The above article is not intended as legal advice because each set of circumstances will differ. Specific legal advice is required for each particular case.

End