BUDDLE FINDLAY

Privacy: what to watch in 2021

Amy Ryburn, Allan Yeoman, Philip Wood, Renee Stiles, Damien Steel-Baker, Keri Johansson, Alex Chapman

9 March 2021

With 2021 now in full swing, we thought it a useful time to take a look at six privacy issues that businesses in New Zealand will want to keep a watching brief on in 2021.

Transfers of information overseas

One of the key changes introduced in the Privacy Act 2020 is the introduction of Information Privacy Principle 12 (IPP12). Under IPP12, agencies can now only disclose personal information to a foreign person or entity who is using the information for its own purposes if one of the conditions in IPP12 is satisfied, the main conditions being that the overseas person or entity:

- Has been authorised by the relevant individual
- Is 'carrying on business in New Zealand' and the disclosing agency believes on reasonable grounds that the foreign person or entity is subject to the Privacy Act
- Is otherwise required to protect the information in a way that, overall, provides comparable safeguards to those in the Privacy Act (eg by way of the Office of the Privacy Commissioner's template model clauses).

The Office of the Privacy Commissioner has recently provided helpful guidance to assist agencies identify whether IPP12 applies and, to the extent it does apply, how to comply with it. Of particular note, the guidance sets out factors that the Privacy Commissioner will consider in relation to 'carrying on business in New Zealand', such as repetitive, systematic or continuing use of personal information in New Zealand, websites targeted at New Zealanders, activities that take place or are acted upon in New Zealand, and the holding of trade marks and registered web domains in New Zealand. As we've noted before, the potential scope of the phrase 'carrying on business' is very broad so this additional clarity is welcome.

Is New Zealand still adequate?

Whether or not New Zealand retains its adequacy status with the EU and now also the UK, remains to be seen. As we've written about previously, under the EU General Data Protection Regulation (GDPR), the European Commission has the power to determine whether a country outside of the EU offers an adequate level of data protection. If a country is deemed to have an adequate level of data protection safeguards in place, then personal data can flow freely between the EU and that country without any other data safeguards required. Following 'Brexit', the UK equivalent of the GDPR has also recognised these adequacy decisions – enabling the continued free flow of personal data between the UK and New Zealand. Without adequacy, the administrative requirements are more onerous for transfers to the EU (and now also the UK). For example, a company that shares data on an intra-group basis between the EU and New Zealand would need to put in place binding corporate rules (which would need to be approved by the relevant supervisory authority in the EU) or enter into a data transfer agreement based on the European Commission's Standard Contractual Clauses – in each case, the data being transferred and the purpose for the transfer would need to be clearly understood, documented and agreed between the relevant parties.

From the Office of the Privacy Commissioner's November briefing to the incoming Minister of Justice, we understand that the European Commission's review into whether New Zealand's data protection laws provide an 'adequate' level of protection for personal data is still ongoing, with assistance being provided by the Office of the Privacy Commissioner and the Ministry of Foreign Affairs and Trade. If adequacy is not maintained, then the European Commission's proposed new Standard Contractual Clauses (which propose considerable changes to the existing Standard Contractual Clauses) will also become of particular importance to businesses in New Zealand. The alternative approach would be to make further amendments to the Privacy Act to align it more closely to the GDPR in the hopes of having adequacy reinstated (although this could take some time).

Consumer data rights

Consumer data rights (CDRs) are a statutory right for consumers to securely share data held about them by agencies with third parties (eg alternative service providers) and are intended to provide consumers with significant benefits, including increased competition and ease of switching providers. CDRs were not included in the Privacy Act (despite the Privacy Commissioner's submissions on the Privacy Bill). However, following on from trends overseas to implement CDRs (eg in the European Union, United Kingdom and Australia), late last year the Ministry of Business, Innovation and Employment undertook a consultation in relation to introducing CDRs in New Zealand. This consultation covered the potential costs and benefits of CDRs and the potential scope and options for implementing CDRs in New Zealand.

The outcomes of this consultation are still unknown but, if CDRs are introduced, this could have a significant impact on the Privacy Act 2020 (particularly given the potential overlap between CDRs and the access rights already set out in principle 6 of the Privacy Act) and indeed on a number of New Zealand businesses who may need to make changes to their operations and technology to give effect to these rights.

---

e-Privacy Regulation

On 5 January 2021, the European Commission released a proposed new draft e-Privacy Regulation for the EU. Once approved, the e-Privacy Regulation will replace the Directive on Privacy and Electronic Communications (Directive 2002/58/EC) and will regulate electronic communications in the EU by introducing and revising rules in relation to, for example, direct marketing, cookies and the confidentiality of communications content (eg emails and text messages) in the EU.

Of particular note, while consent remains the primary basis on which most cookies can be processed, the draft e-Privacy Regulation now introduces a GDPR standard for consent (so that consent must be freely given, specific, unambiguous and given by clear affirmative action). The draft e-Privacy Regulation also requires that individuals must have a genuine choice regarding the cookies they accept – specifically, 'cookie walls would only be acceptable if the individual is able to choose between that offer and an equivalent offer by the same provider that does not involve consenting to cookies. To avoid 'cookie fatigue', the e-Privacy Regulation also provides for an ability for individuals to 'whitelist' providers' cookie settings through their browsers – and software providers are 'encouraged' to make it easy for individuals to set up these whitelists and to enable them to withdraw consent at any time. The draft e-Privacy Regulation has been a long time coming – it was initially intended to apply from 25 May 2018 alongside the GDPR – but there have been various delays while EU member states seek to agree the text of the regulation. In terms of next steps, the text of the e-Privacy Regulation will now need to be negotiated between the Council of the EU, the European Parliament and the European Commission.

The e-Privacy Regulation should be of note for businesses in New Zealand that operate in the EU as, like the GDPR, the e-Privacy Regulation applies on an extra-territorial basis (as the rules apply in relation to individuals in the EU regardless of where the processing takes place) and can attract fines of up to the greater of €20m or 4% of worldwide turnover.

Developments in Australia

In addition to its recent efforts to implement a media code for Google and Facebook (Regulating the news – the battle across the ditch (buddlefindlay.com)), the Australian government (through the Attorney-General's office) is undertaking a review of Australia's Privacy Act 1988 (Cth). The review is wide ranging and the terms of reference include considering the scope and application of the Privacy Act (including the existing employee records and small business exemptions and the scope of the definition of personal information), consent requirements, overseas transfer requirements, data erasure, whether individuals should have direct rights of action to enforce privacy obligations and enforcement powers. Consultation was undertaken by the Attorney-General's office late last year, with a discussion paper expected to be released in 2021 to identify possible options for reform and to seek more specific feedback. The review is expected to result in significant reforms to Australia's privacy laws and, while these reforms may still be in relatively early stages, New Zealand businesses that operate in Australia will need to keep a close eye on how these reforms progress and what operational impacts they may have (particularly if the reforms go further than the rights granted to individuals under the New Zealand's Privacy Act 2020).

Privacy breach notifications

One of the most talked-about changes in the new Privacy Act 2020 (which came into force on 1 December 2020) was the introduction of mandatory privacy breach notifications. Under the new Act, any organisation that suffers a 'privacy breach' will be required to make a notification to the Privacy Commissioner and to affected individuals if it is reasonable to believe that the breach has caused serious harm to affected individuals, or is likely to do so. With data security breaches and hacks becoming more common, it will be interesting to see how agencies in New Zealand and, indeed, the Privacy Commissioner apply the 'serious harm' threshold in the Privacy Act in practice. In this context, the recent guidelines from the European Data Protection Board in relation to identifying and recognising personal data breaches in the EU may also provide useful guidance for agencies in New Zealand

when undertaking risk and harm assessments.

Auckland

188 Quay Street
Auckland 1010

PO Box 1433
Auckland 1140
New Zealand

P: +64 9 358 2555
F: +64 9 358 2055

Wellington

Aon Centre
1 Willis Street
Wellington 6011

PO Box 2694
Wellington 6140
New Zealand

P: +64 4 499 4242
F: +64 4 499 4141

Christchurch

83 Victoria Street
Christchurch 8013

PO Box 322
Christchurch 8140
New Zealand

P: +64 3 379 1747
F: +64 3 379 5659