BUDDLE FINDLAY

2018: The year privacy became mainstream

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

6 December 2018

Earlier this week Renee Stiles and Alex Chapman of Buddle Findlay's TMT team attended the Privacy Commissioner's International Privacy Forum in Wellington. The forum featured a number of international privacy commissioners and regulators, including the UK Information Commissioner (Elizabeth Denham), and highlighted a number of key issues relevant to New Zealand's privacy landscape.

Convergence

There is a movement towards convergence of data protection and privacy laws globally. This reflects that privacy and data protection is becoming mainstream (largely as a result of the Cambridge Analytica breach and several other high profile privacy breaches during the course of 2018) and that there is an increased understanding amongst governments about the importance of strong data processing regimes and ensuring that individuals have access to their personal information. The UK Information Commissioner described this as a "race to the top" amongst countries in terms of the development of privacy and data protection laws.

It will be interesting to see whether this convergence and heightened focus is reflected in the New Zealand Privacy Bill when the Select Committee releases its report on it in March 2019.

Extra-territorial reach of the GDPR

As we've discussed before, the extra-territorial provisions in the EU's General Data Protection Regulation (the GDPR) remain a key concern for New Zealand businesses. In this context, the UK Information Commissioner noted that the European Data Protection Board's draft guidelines on the extra-territorial provisions of the GDPR may be helpful.

While the guidelines are in draft, they provide a useful indication of the likely interpretation of the GDPR's extra-territorial reach. Of particular note for New Zealand businesses will be the commentary in relation to monitoring data subjects' behaviour as far as their behaviour takes place within the EU. The draft guidance highlights that there does not need to be any intention to monitor individuals within the EU for the GDPR to apply. Accordingly, simply tracking individuals through the use of cookies may be enough to bring you within the scope of the GDPR. However, as noted in the draft guidance, “The EDPB does not consider that any online collection or analysis of personal data of individuals in the EU would automatically count as “monitoring”. It will be necessary to consider the controller’s purpose for processing the data and, in particular, any subsequent behavioural analysis or profiling techniques involving that data. The EDPB takes into account the wording of Recital 24, which indicates that to determine whether processing involves monitoring of a data subject behaviour, the tracking of natural persons on the Internet, including the potential subsequent use of profiling techniques, is a key consideration.” Where the line will be drawn is, in our view, likely to be the subject of some debate in the future.

Penalties

In light of the extra-territorial reach of the GDPR, businesses are rightly nervous about the potential penalties that may apply in relation to breaches of the GDPR: a breach of the GDPR can result in penalties of up to 20m Euros, or of 4% of an undertaking's total annual worldwide turnover, whichever is higher.

The UK Information Commissioner stressed that proportionality is embedded into the GDPR and that New Zealand companies 'trying their best' and engaging with EU regulators are unlikely to be subject to penalties under the GDPR regime. Instead, it is likely that regulators will rely on their extensive investigative and advisory powers to ensure that the GDPR is being complied with appropriately. In terms of enforcing penalties, the UK Information Commissioner acknowledged that there may be some practical limitations but that it would seek to rely on assistance from other jurisdictions to ensure that the GDPR was enforced as necessary.

Public interest

A recurring theme amongst the privacy regulators that spoke at the Forum was a substantial increase in both the ability of members of the public to exercise rights in order to control the use and collection of their personal data and public engagement in privacy issues generally - with many referring to 2018 as the year privacy and data security have gone 'mainstream'.

This has led the need for additional resource for privacy regulators, particularly following the introduction of mandatory data breach notifications in the EU and Australia. We note that similar obligations have been proposed in the New Zealand Privacy Bill, although it remains to be seen whether the introduction of such obligations will also see the New Zealand Privacy Commissioner's requests for further funding being realised.

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