BUDDLE FINDLAY

EU-US Privacy Shield, Brexit – where to next for European data protection law?

Allan Yeoman, Keri Johansson

6 September 2016

Arguments amongst UK and European politicians and privacy regulators could be dismissed as irrelevant to this end of the world. But Australian and New Zealand companies who operate in or are eyeing up Europe will need to keep up to speed with a number of recent changes to EU privacy laws.

For those who follow developments in European data protection law, the European Commission's vote to approve the EU-US Privacy Shield on 12 July 2016 may have been somewhat overshadowed by the result of the Brexit referendum just a few weeks earlier.

It had already been a big few months in the world of European privacy law. The General Data Protection Regulation (GDPR), the set of rules which will replace the EU Data Protection Directive, was agreed in December 2015 and will come into force in May 2018. And the Court of Justice of the European Union declared in the *Schrems* decision in October 2015 that the Safe Harbour regime, under which US companies certified compliance with EU-standard data privacy practices, could no longer be trusted and was invalid.

The *Schrems* ruling caused a scramble among US companies whose businesses involve the storage or handling of European personal information to put in place alternative means of meeting EU data protection requirements. For Australian or New Zealand businesses with customers in the EU, inboxes would have been full with urgent requests from US hosting providers, SaaS vendors and other suppliers to sign up to 'Model Clauses' based on the European Commission-approved standard contractual terms for transfers from EU-based data controllers to offshore data processors.

Meanwhile behind the scenes, privacy and trade regulators from the EU and US were working hard to develop a more permanent solution. The result is the Privacy Shield, claimed to be a beefed up version of Safe Harbour with stronger obligations on US signatory companies, clearer rights of redress and inquiry for EU citizens (including a dedicated ombudsperson), and assurances from the US government regarding access to data for law enforcement and national security purposes - an issue central to the *Schrems* decision.

The impact of Brexit

So, given the UK has voted to leave the EU, should we still care what happens to European privacy law over the next few years? Clearly, the answer is yes.

First, Brexit is only relevant, to any degree, to businesses whose European operations are headquartered in the UK, or who use data processing equipment located in the UK. For those with offices or equipment in other EU member states, European privacy law should go on largely uninterrupted, including with reforms as scheduled.

Second, it's unlikely that there will be any substantial change in UK data protection law in the foreseeable future. Brexit has a two-year runway so the English Data Protection Act 1998 and privacy directives from Brussels will remain the law of the land in the short-to-medium term.

Even in the long-term, post-Brexit it seems doubtful that the UK would choose a substantially different path from the rest of Europe. Significant commercial and trading hurdles could emerge if the European Commission found reason to declare UK privacy law 'inadequate', and compliance costs for UK businesses would dramatically increase. The more logical view is that the UK would, in the same way Switzerland has done, maintain a set of privacy laws that it knows to be consistent and harmonised with EU standards, minimising the disruption for UK businesses with customers and trading partners elsewhere in Europe.

However, the timeframe for Brexit means that UK businesses, and Australian and New Zealand companies who need to comply with UK data privacy law, will need to adopt practices compliant with the new GDPR when it is implemented in May 2018. So even as the UK is walking towards the exit, businesses will have to keep up with privacy law reform when the GDPR comes into force, and then re-adjust to whatever post-Brexit privacy regime replaces it.

The upshot is that it should largely be business as usual for Australian and New Zealand businesses in terms of the need for them to comply with European data protection laws. While the demise of Safe Harbour, its replacement with the Privacy Shield, the new

GDPR and Brexit amount to a generation of reform and upheaval in the space of less than a year, it remains as important as ever for privacy compliance to remain near the top of the agenda for those operating in Europe.

This article was written by Allan Yeoman (partner) and Keri Johansson (senior associate) for the Australasian Lawyer magazine (Issue 3.4, August 2016).

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