The global outlook on data protection—the UK

28/05/2019

As part of a series on different data protection regimes across the globe and how UK businesses operate within them, we consider the future of the UK data protection regime as it enters uncertain times. Adam Rose, partner at Mishcon de Reya, discusses the effect that Brexit will have on the Data Protection Act 2018 (DPA 2018), and on UK data protection more generally.

What changes did DPA 2018 bring? Why were they necessary?

DPA 2018 did a number of things. The General Data Protection Regulation (EU) 2016/679 (GDPR)—being an EU regulation—became UK law as an automatic matter on 25 May 2018 and the UK need not have done anything further.

Instead, DPA 2018 did the following: In DPA 2018, part 2, a number of provisions in GDPR—which provided that Member States could choose to implement certain optional aspects—were introduced into UK law. For example, whereas GDPR provided that for online services, a 'child' could be an under-16-year-old or an under-13-year-old, DPA 2018 went with age 13 as the cut-off. A number of other aspects left to the Member State were also introduced in this part of DPA 2018—most notably, various exemptions are set out in schedules 2, 3, and 4. DPA 2018, part 2 could be seen to supplement GDPR.

DPA 2018, part 2 also sets out what is called the 'Applied GDPR'—in effect, it repeats GDPR and applies it to situations where GDPR itself does not apply. For instance, where certain activities fall outside of the scope of EU law.

DPA 2018, part 3 addresses a parallel piece of EU law that came into effect on 25 May 2018—namely the Law Enforcement Directive (EU) 2016/680—which deals with the UK's implementation of law enforcement processing by the police and similar bodies. This was a necessary step for the UK to take, although including these provisions in DPA 2018 possibly further convolutes an already complex piece of legislation. In my view, it would have been easier to have included this as a stand-alone act or statutory instrument (SI).

DPA 2018, part 4 addresses intelligence service processing—that is, the processing of personal data by the security services (MI5, MI6) and GCHQ. This has long been a controversial area, where successive UK governments have sought to enable somewhat broad processing by the intelligence agencies.

DPA 2018, part 5 deals with the role and standing of the Information Commissioner's Office, DPA 2018, part 6 with enforcement, and DPA 2018, part 7 with supplementary provisions.

What changes are being made to the Data Protection Act 2018 in light of Brexit? Why? What is the impact?

Should Brexit happen, references in GDPR to various EU institutions will need to be adapted to reflect UK equivalent bodies, and GDPR itself will need to be brought into UK law with certain amendments to the GDPR and DPA 2018. DPA 2018 didn't bring the GDPR into UK law, as such, as GDPR became directly applicable in the UK on 25 May 2018. Leaving the EU would otherwise cause GDPR to be ineffective in the UK. In order to meet the eventuality of Brexit, Parliament has passed certain SIs that are designed to have the effect of amending the GDPR as it will be incorporated into domestic UK law following Brexit as well as amending the DPA 2018.

What is the likelihood of the UK remaining closely aligned to the EU's GDPR regime after Brexit? How closely should a UK domestic regime reflect the GDPR regime?

Some countries have updated their laws to bring them more in line with GDPR, and the proposal is that the UK will continue to align closely by incorporating GDPR into UK law with amendments, such as to the DPA 2018. This does not mean that they are 'part of the GDPR'.

The more closely aligned a country's laws are with GDPR, the more likely it is that the EU and the European Commission will determine that they are countries that provide a sufficient level (or 'adequate') protection for personal data when it comes to transfers of data.

If it leaves the EU, and the GDPR regime, is there a risk of the UK being left out of a regime which could benefit trade? What would be the effect on UK business?

If the UK leaves the EU, then it will be treated as a 'third country'. As such, data transfers from the EEA to the UK will normally need to be made under cover of the EU's model clause contract terms or another formal transfer mechanism permitted by applicable data protection laws (eg binding corporate rules), rather than, as now, without formality. The EU has indicated that finding the UK able to provide an adequate level of protection is not a priority. In normal circumstances, it would take the EU about two years to make such a determination. Given the UK's membership of the EU until Brexit, one might expect a decision in shorter time, but there is no indication that will happen.

Being a third country would be damaging for those UK businesses that provide any processing services for EU-based businesses—anything that creates a barrier to trade will harm UK business—and risks meaning that multinational companies will start to move processing activities into other EU member states and out of the UK.

In due course, the EU might recognise the UK as providing adequate protection for personal data, simplifying the process of data transfer again. To achieve that, the UK is going to have to offer the EU something to encourage the EU to address the issue. The political declaration on the future relationship which was published alongside the draft withdrawal agreement provides that the EU will 'endeavour' to adopt an adequacy decision in relation to the UK by the end of the transition period. However, as things stand today, getting the withdrawal agreement through parliament doesn't look likely, and in that case, there will be no transition period, and so no urgency to making an adequacy decision.

Interviewed by Tom Inchley.

The views expressed by our Legal Analysis interviewees are not necessarily those of the proprietor.