BREXIT AND DATA PROTECTION: KEEP CALM AND CARRY ON?

Brexit should not distract businesses from their work to prepare for implementation of the EU General Data Protection Regulation in 2018. Reforms are coming with or without Brexit.

It is not yet clear how the UK's vote to leave the European Union will impact data processing and sharing across Europe. Businesses will need to anticipate possible new barriers to data sharing whilst at the same time working to encourage pragmatic solutions. In practice, however, it is unlikely that Brexit will be significantly disruptive from a data protection perspective.

Key issues

- Future UK data protection regime likely to adopt the new EU standards.
- The benefits of "one stop shop" supervision may be lost.
- UK will need to implement an EU-like regime to gain single market adequacy status.
- Business should not be distracted from preparation for the new regime, which is urgent.

EU AND UK DATA PROTECTION LAW

Data protection across the European Union (EU) and European Economic Area (EEA) is regulated by national laws implementing EU Directive 95/46/EC (DP Directive) – in the UK, by the Data Protection Act 1998 (DP Act).

The DP Directive sets standards applicable to processing of personal data across the EU and EEA and restrictions on transfers of personal data to so-called "third countries", outside the EU and EEA.

The DP Directive and DP Act are due to be replaced, as of 25 May 2018, by the new EU General Data Protection Regulation (GDPR), which (for the most part) sets higher data protection standards than the DP Directive and DP Act. As an EU Regulation, the GDPR will take effect across the EU without the need for national implementing legislation. In practice, however, the UK and the other EU member states are working to draft laws to supplement and make exceptions to the GDPR in a number of areas.

The timetable for Brexit is uncertain. The UK could conceivably leave the EU before the Regulation takes effect, but it is more likely to be later. In that case the GDPR will take effect in the UK and then fall away, needing to be replaced by a new UK law. In all likelihood, the UK regime will closely follow the GDPR model.

FUTURE SOLUTIONS

The UK's future data protection regime will depend to some extent on the nature of the UK's wider future relationship with the EU.

If the UK joined the EEA it would be obliged by agreement with the EU to pass a new law effectively implementing the GDPR in the UK. In that case,

therefore, the impact of Brexit on UK data protection regulation would be minimal.

Any other post-Brexit arrangement would be likely to involve some agreement between the UK and the EU. This may or may not involve commitments from the UK regarding its data protection regime – clearly, however, those commitments would not require a higher standard of data protection than the GDPR.

Subject to any data protection commitments that the UK might make to the EU, the UK would in theory be free to regulate data protection post-Brexit as it saw fit.

This freedom would however be more theoretical than real. The GDPR, like the DP Directive, will impose tight restrictions on transfers of personal data from the EU and EEA to other countries which do not ensure an "adequate" level of protection for personal data. The European Commission, with the EU Court of Justice looking over its shoulder, will need to decide whether the UK's new regime ensures an adequate level of protection.

A decision that the UK did not provide an adequate level of protection would be disruptive, putting the UK in the same category as non-EEA countries such as the US, China and India and requiring burdensome administrative steps to be taken to allow data sharing between the EU and the UK to continue.

In practice, therefore, the UK is likely to adopt a GDPR-like level of data protection, so as to ensure that EU and UK businesses can continue to share personal data. The UK Information Commissioner has indicated that this is his expectation (see https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/06/referendum-result-response).

POSSIBLE UK LIBERALISATION?

There may in theory be some scope for the UK to liberalise its future data protection regime.

First, there is the possibility of the UK opting out of the new GDPR standards and asserting that the current regime, embodied in a lightly amended version of the DP Act, provides an "adequate" level of protection. This would somewhat reduce the regulatory burden for UK business. In theory, the UK could also make changes to liberalise the current regime.

The EU Court of Justice however takes the view that, for a third country's data protection regime to be "adequate", it must be at least broadly equivalent to the EU regime (see Schrems v Data Protection Commissioner (C-362/14)). Where the EU has concluded that its current regime is not fit for purpose, and legislated to improve it, it is hard in this context to see how the Commission could conclude that a law based on the old regime delivers adequate protection. This will be an issue for other third countries (such as Argentina, Canada, Israel and Switzerland) already determined by the Commission to ensure an adequate level of protection, and the Swiss authorities, at least, are already considering changes to their data protection laws to anticipate this issue.

A more elaborate possibility would be for the UK to apply two different data protection standards, one based on the GDPR and applying to personal data transferred from the EU or EEA (or available to be adopted on a voluntary basis, like the proposed US "Privacy Shield"); and another, more liberal, standard applying to "domestic" personal data. This approach could, for

example, allow relatively free transfer of UK personal data to the US and elsewhere and give the UK businesses a small competitive advantage over their EU colleagues.

The attractions of this approach are likely to turn out to be more theoretical than practical, however, even if it were permitted by the agreement ultimately reached between the EU and the UK. A dual regime would be complex and difficult to understand and apply, and of course UK citizens would have to be persuaded to accept a lower level of protection of their personal data than would have been delivered by a vote to remain. The Commission would also need to be convinced that the higher standard would be applied in practice to personal data transferred from the EU and EEA, despite the practical difficulties of distinguishing between categories of data in consolidated processing systems.

IMPACT ON "ONE STOP SHOP" PROPOSALS

As we have seen, there is the theoretical possibility of new restrictions on transfer of personal data from the EU to the UK, and of a more liberal regime governing processing of personal data within the UK, but at this stage both seem unlikely.

It is however likely in practice that Brexit will disrupt the so-called "one stop shop" arrangements in the GDPR. Businesses operating in both the UK and the EU will inevitably be regulated by different data protection authorities when they process personal data for the purposes of their EU and their UK operations. There will also be circumstances where both the EU and the UK regimes apply – for example, if a UK business outsources processing to a service provider in Poland – which may create difficulties even if the two regimes are substantively the same.

It is likely in practise that Brexit will disrupt the so-called one stop shop arrangements in the GDPR.

Following Brexit, the UK Information Commissioner will no longer have any formal role in shaping the interpretation and enforcement of the GDPR. The Commissioner's office has a well-won reputation as a moderate and pragmatic force within the European data protection community, so this may lead to less business-friendly approaches in the future.

WHAT TO DO NOW

For the time being, UK and other European businesses need to continue to work to prepare for implementation of the GDPR. Brexit should not be allowed to get in the way of GDPR preparations.

One likely effect of Brexit, in fact, will be a delay in visibility of the detail of the UK's post-GDPR regime. Business has been pressing the UK Government to work quickly to draft the legislation that will be needed to supplement and make exceptions to the GDPR. The need to take account of the consequences of Brexit and the sheer level of distraction created by the vote are likely seriously to delay that process.

Businesses should be prepared to modify their data protection compliance strategies to take account of the peculiarities of a future UK regime, but on the assumption that these peculiarities are likely to be at the margin rather than within the fundamental principles established by the GDPR. So in other words, businesses should keep calm and carry on.

CONTACTS

Richard Jones
Director of Data Privacy

E richard.jones
@cliffordchance.com

Jonathan Kewley
Senior Associate

E jonathan.kewley
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ