

Digital departure

William Long assesses the impact of Brexit on data protection legislation in the UK



William Long is a partner at Sidley Austin

On 23 June 2016, UK voters passed a referendum to leave the European Union (EU) after a membership of nearly 40 years. This historic decision is likely to have a profound impact on political, economic and regulatory decisions in the coming months and years, while politicians negotiate the terms of the UK's exit from the EU. The impact of this decision on many different areas of law and regulation will need to be carefully examined and monitored over the coming months, including in relation to data protection.

Current UK data protection legislation

The protection of personal data in the UK is governed by the Data Protection Act 1998 (DPA), which implements the current EU Data Protection Directive 95/46/EC (the Directive). Accordingly, if the UK withdrew from the EU before May 2018, and so before the recently adopted EU General Data Protection Regulation (GDPR) became law in the UK, the DPA would continue to apply and so the UK would have data protection laws that have EU data privacy principles at their core. Indeed, the UK's Information Commissioner's Office (ICO) confirmed, following the referendum result, that the DPA 'will remain the law of the land'. However, the DPA came into force almost 20 years ago and is therefore relatively out of date in the modern digital world.

Impact of Brexit on the implementation of the GDPR

The GDPR was expected to take effect in the UK by 25 May 2018.

As the GDPR is an EU regulation, it is directly applicable in all member states. Whether it remains directly applicable to the UK will depend on how quickly the UK serves its notice under Art 50 of the Lisbon Treaty and how quickly a withdrawal agreement can be negotiated. Unless a withdrawal agreement can be negotiated and unanimously agreed in under two years, it is unlikely that the UK will have left the EU before the GDPR comes into force. Accordingly, in this circumstance, the GDPR will apply in the UK from 25 May 2018 and therefore UK organisations, and organisations that operate across the UK and the EU, should continue with their GDPR preparations, an approach confirmed by the ICO.

Even if the UK was to leave the EU shortly after the GDPR comes into force, due to the extra-territorial scope of the GDPR, any UK business that processes personal data of EU citizens either:

- through offering goods or services to such citizens; or
- by monitoring their behaviour (monitoring includes tracking information about data subjects, such as their preferences, attitudes or behaviours),

will need to comply with the requirements of the GDPR.

Therefore, at least for the short term, Brexit may have minimal impact on the applicability of the GDPR, as it is very likely to be directly applicable in the UK before the UK leaves the EU and in any event many organisations

'If the UK was to adopt its own data protection rules and regulations, it would likely ensure that these comply with EU data protection laws, in order to obtain an adequacy determination from the European Commission.'

in the UK will still come within its scope even after the UK leaves the EU. Indeed, the ICO has said it will be speaking with government to present its view that reform of UK data protection law still remains necessary, given the need for clear laws and safeguards in the growing digital economy.

However, what happens following the UK's exit from the EU is still uncertain and varies depending on the type of deal agreed between the UK and the EU. This uncertainty was acknowledged in a speech delivered on 4 July 2016 by Baroness Neville-Rolfe, the UK Minister for Data Protection. Neville-Rolfe stated that:

We do not know how closely the UK will be involved in the EU system in the future. On one hand, if the UK remains within the single market EU rules on data might continue to apply fully in the UK. On other scenarios we will need to replace all EU rules with national ones. Currently

it seems unlikely we will know the answer to these questions before the withdrawal negotiations get under way.

The impact of the potential relationships with the EU

One of the options for maintaining a relationship with the EU post Brexit

with certain EU regulations and restrictions that are contained in the EEA Agreement negotiated as part of EEA membership. The Directive was implemented into local laws by each member of the EEA, and it is expected that the GDPR will apply to members of the EEA. Therefore, if the UK chose this option, the impact

What happens following the UK's exit from the EU is still uncertain and varies depending on the type of deal agreed between the UK and the EU.

is for the UK to remain part of the European Economic Area (EEA). Being part of the EEA will allow the UK to benefit from continued use of free trade agreements, including being part of the EU single market. The downside of this arrangement is that the UK would have to commit to complying

on data protection legislation would be minimal, as the GDPR would be directly applicable in the UK.

The UK could also choose to follow the Swiss model and become a member of the European Free Trade Area (EFTA). This would mean that the UK has access to the single market through a regularly updated bilateral

PROCUREMENT & OUTSOURCING JOURNAL

The bi-monthly journal designed to meet the needs of procurement professionals

Each issue:

- ▶ Provides up-to-date information on all aspects of procurement law and practice
- ▶ Reports authoritatively on recent case law
- ▶ Opens a forum for discussion by procurement professionals
- ▶ Contains updates for managers, practitioners and procurement authorities



**For a FREE sample copy: call us on
020 7396 9313 or visit www.legalease.co.uk**

agreement with the EU. Under this model, the UK would be free to create its own laws; therefore in theory, the UK could tailor-make its data protection laws and potentially exclude the more stringent provisions of the GDPR and/or the Privacy Shield (see below). Although, as mentioned, UK businesses with personal data on EU citizens would still be subject to the GDPR due to its broad extra-territorial application.

receives from EU member states will not then be transferred to the US on less stringent terms, as this could be an important part of any adequacy determination from the European Commission. An adequacy determination means that a jurisdiction adequately protects the data protection rights of EU citizens and therefore has incorporated EU-strength data protection laws. According to Neville-Rolfe, a

interpretation, approving codes of practice and being on the appellate board in GDPR disputes.

The ICO has a reputation for being more business-friendly than other EU regulatory authorities, and its opinions have always been regarded highly. The Brexit vote is likely to have significantly diminished the weight given to the opinion of the ICO, making it difficult for the ICO to have an impact in the lead-up to the GDPR coming into force. Furthermore, unless the UK can negotiate a position for the ICO on the EDPB (which is unlikely given that the EDPB is to be made up of representatives from EU member states), the ICO will have no voice over issues that relate to the GDPR or other key data protection issues.

The Brexit vote is likely to have significantly diminished the weight given to the opinion of the ICO, making it difficult for the ICO to have an impact in the lead-up to the GDPR coming into force.

International transfers of personal data

Under the Directive and the GDPR (once in force), there is a general prohibition on the transfer of personal data to countries outside the EEA, which do not ensure an adequate level of protection, such as the US, unless certain exemptions apply. Up until October 2015, one of the ways in which personal data could be transferred from the EU to the US was for US companies to self-certify under the US-EU Safe Harbor scheme. However, following the ruling in *Maximillian Schrems v Data Protection Commissioner* [2015] by the Court of Justice of the European Union, the EU-US Safe Harbor framework was declared invalid and negotiations were concluded in respect of an alternative transatlantic data transfer framework, the new EU-US Privacy Shield, on 12 July 2016, with applications for certification possible from August 2016.

However, there is uncertainty as to the impact Brexit will have on the EU-US Privacy Shield. For example, could departure of the UK from the EU lead to the development of a UK-US framework for data flows that is less onerous than the highly rigorous EU-US Privacy Shield? This is questionable, as the UK is likely to have an incentive to demonstrate to the EU that the data flows it

determination of adequacy 'will be a major consideration in the UK's negotiations going forward'. Accordingly, if the UK was to adopt its own data protection rules and regulations, it would likely ensure that these comply with EU data protection laws, in order to obtain an adequacy determination from the European Commission.

The impact on the ICO

Brexit may also have a significant impact on the role of the ICO, the UK's national regulatory body. The ICO is a member of the Article 29 Working Party, which includes representatives from each EU member state's regulatory authority and offers advice and opinions on data protection issues. The Article 29 Working Party has already been very influential in the drafting of the GDPR, as well as the drafting of the Privacy Shield. It is also anticipated that the Article 29 Working Party will play a significant role in the lead-up to the implementation of the GDPR, offering opinions, advice and guidance on the interpretation of its provisions.

Once the GDPR is implemented, the Article 29 Working Party will be replaced by the newly formed European Data Protection Board (EDPB). The EDPB is intended to play an important role in ensuring GDPR compliance, offering guidance on its

Conclusion

We are currently in a period of uncertainty, making it difficult to determine the full impact of Brexit on data protection regulation. In the short term, there is likely to be little change in the data protection landscape, and UK organisations should continue with their preparations for the implementation of the GDPR. Despite this inevitable short-term uncertainty and confusion, we may also be looking at a possible silver lining in the longer term. The loss of the UK could help focus the EU to come good on its commitment to promote Europe's digital economy where businesses can thrive without over-regulation. With that, we could actually see greater international convergence on regulatory policy and a move towards a more reasonable approach to harmonisation of privacy laws. In addition, the UK not being directly subject to EU regulation may over time cause it to be seen as an attractive place for innovative companies and technologies to develop. In the meantime, however, we will have to wait and see how the aftermath of the referendum unfolds and the outcome of negotiations with the EU. ■

Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* (2015) Grand Chamber, 6 October