

Data privacy and Brexit—deal breaker or opportunity to reboot?

26/01/2017

IP & IT analysis: What impact might the forthcoming Brexit negotiations have on data privacy in the UK? As part of a series of articles to mark Data Privacy Day, Ian Whitehurst, Barrister at 6 Pump Court and 7 Harrington Street, considers the potential impact of Brexit on data protection issues.

What effect might Brexit have on data protection and how is it likely to affect existing UK rules?

In the UK, the regulation and protection of personal data is presently primarily governed by the Data Protection Act 1998. Brexit will not affect this piece of primary national legislation.

Furthermore, the government has confirmed that the General Protection Data Regulation, [Regulation \(EU\) 2016/679](#) (the GDPR), which will become the new template for data protection and regulation across the EU, will apply to the UK from 25 May 2018. EU Member States are not required to deploy national measures to transpose or implement the GDPR.

Once the UK is out of the EU, it will no longer be bound by EU law, but until that time it will remain subject to EU law and the jurisdiction of the EU courts. Once Brexit is triggered under Article 50 TEU, the UK will have to negotiate the terms of withdrawal from the EU and legislate accordingly. It is believed that the process may take up to two years and thus Brexit may only be achieved after the GDPR has come into force and has been applied in the UK for some period of time.

Once the UK has completed Brexit, the GDPR will not automatically be part of UK law. However, the government is proposing legislation to adopt and incorporate existing EU law into UK domestic law at the point of exit. It would then be up to Parliament to decide whether to keep or amend the EU-derived law in the UK. Until the Bill is published, we cannot say whether it will include the GDPR, however, if Brexit is to be seen by some as providing an opportunity to change the data protection laws in the UK, that approach would ignore the purpose and jurisdictional remit of the GDPR.

The policy behind the GDPR is to ensure international consistency when dealing with data protection issues and to ensure that any business or service either based in the EU or trading with its Member States complies with its obligations and duties under the regulation. UK businesses will have to comply with the regulation.

In conclusion, due to the need for businesses and individuals to be regulated by internationally consistent data laws, I do not believe Brexit will have any meaningful impact on the existing UK data laws.

What options are available to the UK—could Brexit prove an opportunity to loosen data protection standards and how would it affect implementation of the upcoming GDPR?

Due to the international and cross-border nature of business in today's world and the far reaching jurisdictional ambit of the GDPR, the process of Brexit itself will present little or no opportunity to loosen the data protection standards which are presently applicable in the UK.

The main domestic statute as indicated above will remain in force and the GDPR will apply to companies based outside the EU which offer goods or services to individuals located in the EU.

While the provisions of the GDPR will not technically have to be incorporated into post-Brexit UK law, UK companies trading within the EU will have to ensure that they are compatible and compliant with its duties and obligations.

It is worthwhile to note that the GDPR is likely to be perceived as the 'gold standard' around the world and it would be in the UK's interests to be at the forefront of data compliance and regulation.

Continuing the view from a commercial perspective, allowing for an equivalent level of data protection across borders would ease data transfers into the UK and continue to promote the interests of the UK technology industry. As outlined above, a piece of national legislation mirroring the provisions of the GDPR is almost inevitable.

Could the World Trade Organisation (WTO) approach grant the UK more flexibility with regards to data protection or are there potential stumbling blocks to its ability to transfer data and provide an ‘adequate’ level of protection?

The WTO’s flexible approach may seem superficially attractive but, as the EU will remain a substantial trading bloc that the UK will have to trade with, the provisions and remit of the GDPR will require all UK companies to be compliant with its provisions if they wish to continue to trade with their European business partners.

It would not be practicable for companies to operate a two tier system in relation to data protection. The ‘stumbling block’ for the UK is the growing internationalisation of data regulation legislation.

A further issue is if the UK has a materially different regime to the EU, then the UK will be in a position similar to the US, for which businesses have to go through onerous steps to demonstrate data protection compliance. This is a clear barrier to trade and thus demonstrates why there is a significant commercial benefit for the UK to align itself with the GDPR.

What possible impact might the personal data provisions in the Investigatory Powers Act 2016 (IPA 2016) have on these matters? Is it likely to face a challenge in the courts?

The legislation is known as the ‘Snooper’s Charter’ as it enables the government and the security services on their behalf to obtain information about an individual’s web history and call data without a warrant as well as placing on a legal footing the process of bulk hacking and bulk data collection which now requires the use of a warrant issued by a judge.

As this is a domestic piece of legislation, Brexit will have no material impact upon its provisions. The ability to procedurally challenge this piece of legislation through the courts may be affected by Brexit, as the right to appeal to the Court of Justice of the European Union will be removed once Brexit is enacted. Although, the right to appeal to the European Court of Human Rights will remain.

The nature of the challenge to this piece of legislation will ironically be founded upon human rights and European rights based jurisprudence—issues relating to the right to privacy, a right to a family life and issues of proportionality concerning the actions of government agencies will be at the forefront of the legal challenges.

As there was little political debate about this piece of legislation and its ambit, I expect that there will be considerable ‘rights-based’ challenges in the courts in the near future with parties seeking, for example, rulings on its validity and compatibility with existing European principles and freedoms. Cases C-203/15 and C-698/15: *Tele2 Sverige AB v Post-och telestyrelsen*; *Secretary of State for the Home Department v Watson and others* [2016] All ER (D) 107 (Dec)

On a comparative analysis with the judgment of the Court of Justice on the provisions of the Data Retention and Investigatory Powers Act 2014 (DRIPA 2014), the court ruled that the general and indiscriminate retention of emails was unlawful.

Given the fact that many of the powers contained in DRIPA 2014 are replicated in IPA 2016, the Court of Justice judgment casts doubts on the long term validity and sustainability of IPA 2016.

In order for the UK to continue to be seen as an equivalent regime for data transfers once (or if) Brexit is completed, this issue will have to be urgently addressed.

Any other trends/developments in this area worthy of mention?

On a global level, there is an increase in state surveillance (including limits on the use of encryption technologies by businesses and individuals) and the IPA 2016 is part of that drive by individual governments.

However, the EU is committed to protecting and promoting greater privacy rights and a higher ethical standard for businesses in their observance of such rights by promoting privacy and ensuring greater compliance with data protection laws.

These two factors are in direct conflict with one another and a post-Brexit UK may need to choose which side it is on. This is not an easy choice, but it would seem that any attempt to satisfy both competing interests at once would fail.

This cannot be allowed to happen as the digital economy in the UK is a vital, strong and integral component of the overall national economy which needs to be developed in order to continue the economic success of the UK in a post-Brexit world.

Interviewed by Alex Heshmaty.

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



CLICK HERE FOR
A FREE TRIAL OF
LEXIS®PSL

[About LexisNexis](#) | [Terms & Conditions](#) | [Privacy & Cookies Policy](#)
Copyright © 2015 LexisNexis. All rights reserved.