SQUIRE PATTON BOGGS

Brexit – What Next for Data Privacy in the UK?

The UK electorate has voted to leave the EU. What is the likely impact on the data privacy obligations of UK businesses?

Immediate Impact

The vote for Brexit is of no legal effect per se. It is merely an instruction to the UK government to withdraw from the EU. Withdrawal involves a number of formal steps, beginning with the UK notifying the EU of its intention to withdraw under Article 50 of the Treaty on European Union. Current indications are that this will not happen until a new Conservative Party leader has been elected. The UK and the EU must then negotiate the terms of the UK's exit, which is likely to take a minimum of two years. Nothing will change until the UK actually leaves the EU. That means businesses must, for now, continue to comply with the Data Protection Act 1998 (DPA) and the E-Privacy Regulations. They should also anticipate, and prepare for, the more stringent data privacy regime which will be introduced by the General Data Protection Regulation (GDPR). Businesses must comply with the GDPR from 25 May 2018.

The Longer Term

The effect of the UK's exit from the EU on data privacy obligations will depend on what the UK and the EU negotiate as the alternative to EU membership. There is considerable uncertainty around this at the moment. However, three exit models appear to be the main options.

Option 1 - Norway Model

The UK could become a member of the European Economic Area (EEA), joining Iceland, Norway and Liechtenstein. The UK would have full access to the EU single market but remain subject to many of the EU's fundamental rules and laws, including the Data Protection Directive and the E-Privacy Directive. If this model was chosen, very little would change in practice. Businesses would have to continue to comply with the E-Privacy Regulations and the DPA, until it was replaced by the GDPR from 25 May 2018. Personal data could also be transferred freely between the UK and the EU.

Option 2 – Swiss Model

The UK could opt to negotiate access to the EU single market via a bilateral trade agreement with the EU, in the same way as Switzerland. Again, the E-Privacy Regulations and the DPA would continue to apply. Switzerland has implemented the Data Protection Directive into its national law. As a result, the European Commission recognises Swiss law as providing adequate protection for personal data and on that basis has approved transfers of personal data between Switzerland and the EU. If the UK chose the Swiss model, the UK would become a third country and an adequacy decision would be needed for data to flow between the EU and the UK. Such a decision would probably only be forthcoming if UK law was closely aligned with that of the EU. In other words, once the GDPR begins to apply in the EU, it is likely that the UK would need to implement laws which mirror it (or agree to be subject to the GDPR itself). This makes it likely that, if the Swiss model was chosen, businesses would be subject to the DPA, and subsequently the GDPR, in the same way as now.

Option 3 – Independent Model

The UK could choose to go it alone and independently negotiate its own freestanding trade agreements with the EU and other countries. Although in theory the UK would be free to repeal the E-Privacy Regulations and the DPA, this is highly unlikely to happen in practice. If they were repealed, the European Commission would certainly not issue an adequacy finding in relation to the UK (meaning that there would be considerable legal obstacles to transfers of personal data from the EU to the UK). In the absence of such laws, individual transfers of personal data could take place if, in very limited circumstances, a derogation applied, or there were an alternative means of ensuring adequate protection approved by the European Commission. The options, however, are relatively limited. Currently, they comprise: (i) adopting binding corporate rules, a costly process taking many months; (ii) negotiating a bespoke agreement and getting it approved by a national regulator, also expensive, or (iii) concluding model clauses, but the latter is the subject of challenge through the European Court of Justice. Given the EU's adoption of the GDPR, the European Commission is likely to require the UK to put laws more stringent than the DPA in place as a condition of recognising the adequacy of the UK's data privacy regime. The result could well be that, even if the go-it-alone route was chosen, UK businesses could, in practice, still be subject to the DPA or, more likely, the GDPR, or provisions very similar to it.

The UK Information Commissioner (ICO) in an official statement has said that he believes UK law will need to provide equivalent protection to that of the GDPR, and will be making this case to the government.

Impact of the GDPR

Even if the terms of the UK's exit from the EU do not require it to comply with the GDPR, the extra-territorial nature of the GDPR means that many UK businesses trading in the EU will be subject to it in any case. Specifically, UK businesses that process the data of EU citizens in the course of offering them goods or services (whether paid for or free) or monitoring their behaviour (including for behavioural advertising purposes) must comply with many of the GDPR's obligations and will be subject to the increased fines.

Whatever happens post the UK's exit from the EU, the timing dictates that there is a strong possibility that UK businesses could be subject to the GDPR before the UK leaves the EU, assuming that the Brexit negotiations last for at least two years from the date on which the UK government formally requests to leave the EU. The GDPR, therefore, will become applicable during that negotiation period. The question of enforcement by the ICO remains an open question, but he has stated that he has always worked closely with regulators in other countries, and that would continue to be the case.

A particular area of uncertainty, however, will be for multinational businesses with European operations, having their European headquarters in the UK. They may find that, for their European operations, they are answerable to a continental European regulator and not the ICO.

What Now?

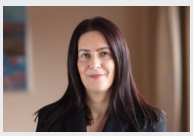
Every business should continue to comply with the DPA (or, if it is non-compliant in any areas, ensure that this is addressed). If your business involves offering goods or services to EU consumers, or you monitor them (for example, by behavioural advertising), you will be caught by the GDPR in any event, and need to start preparations now. For all other UK businesses, it is highly likely that post-Brexit, they will need to comply with the GDPR (or a regime that mirrors it). They too should begin preparing for the coming of the GDPR.

Key Initial Priorities:

- Carry out a data mapping process to create records of what personal data is used by the business, how and why it is used, who it is disclosed to and where and for how long it is stored. This will enable you to carry out a gap analysis, so that you can focus your efforts on any high risk areas of non-compliance and, at the same time, put you in a good position to prepare the business for compliance with the record-keeping requirements of the GDPR.
- Review and revise agreements with third parties and, in particular, with processors, to ensure that you incorporate current and future mandatory and highly desirable requirements. This will ensure that you are compliant, whatever the long term data protection position.
- Ensure you have a robust data breach response plan. This will minimise the chances of a data breach becoming a PR disaster, and enable you to comply with both current and future data breach reporting requirements.
- Review any consents you have for the use of personal data, and what you tell individuals in obtaining those consents, as these are already an increasing area of focus for the UK Information Commissioner, and will be more so under the GDPR.

To discuss the data privacy implications of Brexit for your business, please feel free to call:

Caroline Egan
Consultant
T +44 121 222 3386
E caroline.egan@squirepb.com



Francesca Fellowes
Senior Associate
T +44 113 284 7459
E francesca.fellowes@squirepb.com

Ann LaFrance
Partner
T +44 207 655 1752
E ann.lafrance@squirepb.com