ALLEN & OVERY

Brexit – legal consequences for commercial parties

Data protection legislation – is a change of approach required?

March 2016

Issue in focus

Protecting the privacy of individuals has become increasingly important as awareness of the risks, and the volume of personal data processed, both continue to increase. We are at an interesting time for data protection legislation in the EU.

The existing EU Data Protection Directive, implemented in national law by each Member State, will almost certainly be replaced in 2018 by a new, recently agreed General Data Protection Regulation (the GDPR), which will be directly applicable. This contains some fairly onerous new obligations on those who process personal data, and potentially huge fines for failure to get it right. Data protection has, as a result, been catapulted into the board room and companies are already planning for compliance with the requirements.

At the same time, the current mechanisms for transferring data outside the EU (which are based on a similar toolkit under the GDPR) are under scrutiny. The Safe Harbor regime, which permitted certain transfers to the U.S., was recently declared invalid and national regulators are examining its proposed replacement, the "Privacy Shield". They are also re-considering whether other compliance actions are subject to the same flaws as Safe Harbor.

Although data protection is cited at times as an example of "red tape", we do not think that a Brexit would necessarily change the level of data protection expected of companies processing data in the UK to any significant degree. As a matter of policy, UK law would be likely to impose a broadly equivalent level of data protection to that agreed in the GDPR, at least for personal data transferred to or from the EU, if only to avoid (in the long term) the UK putting in place a similar mechanism to the Privacy Shield, or the need for UK companies to adopt other compliance actions, to enable data to be transferred to them.

From a practical point of view, many multinational companies also find it more convenient to put in place policies and procedures that are consistent across the countries in which they operate. If the UK were to adopt looser standards, this would be unlikely to affect their approach to compliance in the UK. Brexit would, however, result in UK companies that operate in Europe no longer being able to have the UK data protection regulator (the ICO) as its lead supervisory authority in the EU.

Analysis

What is the current position?

The processing of personal data (that is data about identifiable living individuals) is currently regulated at an EU level under the Data Protection Directive 95/46/EC. As a Directive, this instrument had to be implemented in each EU Member State. It was implemented in the UK through the Data Protection Act 1998. The drawback of a Directive (as opposed to the GDPR which, as a Regulation, has direct applicability without the need for local implementation) is that inevitable differences have arisen across Member States in certain areas. These differences include, for example, the sanctions that can be imposed for breaching the legislation, and whether the local data protection authority must be notified in certain circumstances (eg in the event of certain international transfers). This has made it difficult for companies that operate across the EU to adopt a common compliance framework in all relevant Member States.

In recognition of this lack of harmonisation, in an effort to bolster the rights of data subjects, and bearing in mind the huge technological advances of the last 20 years and the vast amount of data being processed, the EU has now agreed a new data protection framework for the EU - the GDPR. This was finally agreed after four years of negotiation in December 2015, and we expect it to be in force across the EU from mid 2018.

While the GDPR is broadly similar in many areas to the current law, it contains some radical changes. These include a raft of new accountability obligations (including obligations to keep records of processing and conduct impact assessments for more risky processing), much higher fines for breach (in some cases up to 4% of annual worldwide turnover) and new data breach reporting obligations for all companies.

A welcome change is the increase in harmonisation across the EU and a "One Stop Shop" mechanism. The "One Stop Shop" means that where a company has a presence in more than one Member State it will be supervised by one lead authority. This lead authority will work with other concerned authorities where necessary to enable a more consistent approach to compliance.

Companies are already starting to analyse and implement the new requirements. Further information about the GDPR is available in our publication "The EU General Data Protection Regulation is finally agreed".

The mechanisms for the transfer of personal data from the EU to other countries are very similar under the GDPR and the existing Directive. However, there is fresh uncertainty in this area. This follows the decision by the Court of Justice of the EU (CJEU) that the Safe Harbor regime (which permits the transfer of data from the EU to participating companies in the U.S.) is invalid. A key factor was the extent of the ability of law enforcement agencies to access personal data transferred from the EU, and the possibility of mass, indiscriminate access which is not considered compatible with EU data protection laws. Another concern was the lack of redress in the U.S. for data subjects. The latest UK proposals for an Investigatory Powers Bill to allow certain monitoring and retention of communications data by UK law enforcement and intelligence agencies have been similarly criticised as not doing enough to protect privacy.

This CJEU decision has also led to other, frequently used methods of transferring data out of the EU being re-assessed. These include the use of Model Clauses (standard contractual clauses approved by the European Commission) and the use of Binding Corporate Rules for intra-group transfers (BCRs). In February 2016 a new framework for transatlantic data flows known as the "Privacy Shield" was agreed at a political level to replace Safe Harbor. However, pending review of the detailed proposals by the Article 29 Working Party (composed of representatives of the national data protection authorities, the European Data Protection Supervisor and the European Commission), the validity of the proposed Privacy Shield remains unclear and other methods of compliance are under threat.

Where would we be left following Brexit?

Many countries outside the EU have looked to the EU for an approach on which to model their own legislation, so EU data protection law is, in some senses, a benchmark for regulation of data processing. Similar legislation has been adopted, for example, in Argentina, Mexico, Switzerland, Israel, South Africa and New Zealand. Experience shows that a lack of harmonisation across Member States is not welcomed by multi-national companies even where the rules in a particular country may be more lenient. It is easier to have consistent rules everywhere and set the compliance level to the highest bar. Therefore it is likely that those companies will continue to comply with the new GDPR framework whether or not there is a Brexit.

In order to participate effectively in the free internal market with the EU in respect of personal data, the UK might seek to have in place a solution which the EU would recognise. This might be achieved by:

- becoming a member of the EEA; or
- seeking to become an "adequate jurisdiction" through a European Commission decision.

European Commission adequacy decisions either apply to the country as a whole (eg New Zealand and Israel) or to selected sectors or regimes (eg those companies in Canada that are subject to the PIPED Act, and, in the U.S., previously Safe Harbor). Adequacy decisions can take many years and it could therefore take some time to achieve this status, depending on the political climate and the regime the UK adopts.

Each of these options would require that the UK data protection legislation demonstrates an adequate level of protection of personal data transferred from the EU. The CJEU Safe Harbor decision stressed that any finding that a country is adequate requires it to provide a level of protection essentially equivalent to that guaranteed within the EU. This raises the bar for future adequacy findings. It is therefore unclear how far the UK could go in changing aspects of the GDPR and still be considered adequate/equivalent. For example, would the UK have to impose a substantially similar sanctions regime? The UK's approach to the Investigatory Powers Bill will also have an impact on adequacy. One possibility would be that the UK would retain the existing Data Protection Act but impose higher standards to meet the requirements of the EU for EU data only. The UK adopted this approach for the exchange of police information with the EU.

The protracted U.S./EU Commission negotiations on the Privacy Shield are an example of the type of regime that the UK could seek to put in place with the U.S.. If the UK seeks to be an "adequate jurisdiction" for transfers from the EU, there may well be restrictions on onwards transfers. The EU would resist any possibility of the UK becoming a weak link in its controls over the transfer of personal data to non-EU countries.

If a structural solution was not put in place, companies would have to look to the other mechanisms or derogations under EU law in order to transfer personal data from the EU, such as Model Clauses or obtaining consent.

One key impact of a Brexit, even if equivalent rules were put in place in the UK, would be that companies processing personal data in the UK would not be able to benefit from the "One Stop Shop" mechanism and may therefore face a differing investigation and sanctions regime from the ICO in the UK than from their EU lead data protection authority. Those who had hoped their lead authority under the GDPR regime would be the ICO would be left disappointed. In the circumstances of a Brexit, such companies may see added advantages in the adoption of BCRs. UK companies (like those in any non-EU jurisdiction) that are included in the BCRs approved by an EU data protection authority, would be an adequate destination for personal data transferred intra-group from the EU.

Other issues would need to be addressed which are common to other specialist papers in this series. For example, a mechanism may need to be put in place to take account of future CJEU decisions. There would also be a need for a transitional period following a Brexit, particularly given the likelihood of protracted negotiations on whether the UK gains an "adequate" status, to ensure that data flows could continue while the new arrangement was being put in place.

What does this mean for you?

We will have to wait and see what a Brexit would mean with respect to data protection regulation. The result would most probably mean little change for companies processing personal data in the UK at least in the short to medium term. It is most likely that some form of equivalent legislation to that which applies to the EU Member States would continue to apply, at least for data transferred to and from the EU, whether through the UK becoming part of the EEA or looking to be declared an "adequate jurisdiction" by the European Commission. Many companies operating across multiple jurisdictions will feel that the best course of action is therefore to continue to prepare for the GDPR in the expectation that even if the UK did leave the EU, a data protection regime which imposes similar requirements to those in the GDPR would be likely to apply.

While we have endeavoured to identify possible scenarios in this note, the position is, at least for the time being, unclear. We will be keeping this under review.

This article is one of a series of specialist Allen & Overy papers on Brexit. To read these papers as they become available, please visit: www.allenovery.com/brexit

Your Allen & Overy contacts

Jane Finlayson-Brown
Partner
Corporate – London

Contact

Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

Charlotte Mullarkey
Senior PSL
Corporate – London

Contact

Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com

Nigel Parker
Partner
Corporate – London

Contact

Tel +44 20 3088 3136
nigel.parker@allenovery.com

David Smith
Special Adviser
Corporate – London

Contact

Tel +44 20 3088 6842
David.a.smith@allenovery.com

If you would like to discuss the issues raised in this paper in more detail, please contact Jane, Nigel, Charlotte or David or your usual Allen & Overy contact.