Browne Jacobson

Brexit: what now for the UK's data protection position?

At the time of writing Theresa May is still Prime Minister but has just suffered a crushing defeat in parliament to her deal for withdrawing from the European Union and faces the prospect of a “no confidence motion” today.

21 January 2019

At the time of writing Theresa May is still Prime Minister but has just suffered a crushing defeat in parliament to her deal for withdrawing from the European Union and faces the prospect of a 'no confidence motion today.

In the hubbub and drama of UK politics (John Bercow’s call for *“Order”* above the din of the voting chamber, the *“ooooh”* of the politicians as the votes were read out) it’s easy to forget that – failing another solution, events triggered in 2016 mean that on 29th March the UK will be outside the European Union.

What does that mean for data protection law in the UK? In particular what about cross border arrangements? Those are the questions that this article seeks to answer.

(Spoiler alert – the table at the end summarises the position for a “no-deal” Brexit)

The impact of a “no deal” Brexit scenario on applicable law and cross border data transfers

In December 2018, the UK Information Commissioner’s Office (ICO) and the UK government issued guidance on the impact of a possible no-deal Brexit on data protection law and practice (the Brexit Guidance).

That guidance will be relevant to all businesses in the UK to whom the GDPR currently applies. However, in the event there is an international element to an organisation’s data processing activities, the guidance will be particularly relevant and should be carefully considered in preparation for Brexit.

The guidance includes practical steps and suggestions for how to approach compliance following Brexit. The ICO focusses in particular on ‘taking stock’, understanding your business and data flows and ensuring that organisations are compliant under the current law, particularly as regards any cross border transfers, as that will assist with addressing any issues following Brexit.
We have summarised the key points relating to the applicable law and cross border data transfers that will have a practical impact for organisations in this article.

What law will apply?

The law

The General Data Protection Regulation (GDPR), as a regulation, applies directly to all member states of the European Union (EU). The UK Data Protection Act 2018, currently in force also incorporates the GDPR and deals with the derogations specific to the UK.
When the UK is no longer a member state of the EU, the GDPR will no longer automatically directly apply to the UK, although the Data Protection Act 2018 will continue to apply.

The UK Government has made clear that EU law currently applicable to the UK, including the GDPR, will be incorporated into UK law post-Brexit as a result of the EU Withdrawal Bill.

The Brexit Guidance similarly confirms that the GDPR is intended to be incorporated into UK law, with necessary changes to deal with UK specific issues and to remove anything which is EU specific (including those provisions relating to the UK's membership of the EU). The UK will therefore have a similar law in place to the GDPR but tailored to the UK (the UK GDPR).

One of the key aspects of the GDPR is its extra-territorial effect. Post Brexit, in addition to the UK GDPR, the EU version of the GDPR will therefore also continue to apply to those controllers and processors in the UK who:

- Process personal data in the context of an establishment in the EU;
- Offer goods and services to individuals in the EU; or
- Monitor the behaviour of individuals in the EU.

The Brexit Guidance confirms that the UK GDPR will have similar extra-territorial provisions relating to an establishment in the UK, offering goods and services in the UK and monitoring the behaviour of individuals in the UK.

What guidance and case law will apply?

As a member state of the EU, the ICO takes into account the guidance of the European Data Protection Board, the EU body in charge of the application of the GDPR, (EDPB) when drafting its own guidance and making decisions. Historically, the ICO has waited for the guidance of the EDPB before drafting its own guidance.
EDPB guidance also provides useful clarification for organisations on key data protection issues.

The EDPB is a made up of the head of each supervisory authority and the European Data Protection Supervisor. The ICO currently sits on the EDPB and plays a part in forming that guidance, representing the interests of UK businesses in doing so.

Following Brexit, the ICO will no longer sit on the EDPB. The Brexit Guidance clarifies that the ICO will seek to maintain a strong relationship with EDPB after Brexit however it is unclear how much influence the ICO will continue to have on the direction that the EDPB takes in its guidance.

If the guidance of the EDPB does not sufficiently take into account UK interests there is a risk that the gap between the approach of the ICO and the approach in the EU will widen.

Case law also often includes useful guidance for approaching the interpretation of the applicable data protection law. In the UK, that currently includes decisions of the UK courts and of the European Court of Justice (CJEU). Although the Brexit Guidance does not address this point specifically, the UK Government has previously said that the UK will not continue to be subject to the jurisdiction of the CJEU after Brexit. CJEU decisions made before Brexit will however continue to apply. The likelihood is therefore that emphasis will continue to be placed on CJEU decisions after Brexit.

In summary

Organisations in the UK that operate in both the UK and the EU will be subject to both the EU and the UK versions of the GDPR and must comply with both laws going forwards. That is unlikely to be an issue to the extent that the laws remain similar, however in the event that guidance and case law leads to different interpretations of those laws, organisations could be in the difficult position of being required to comply with conflicting laws.

International Transfers

What happens if a UK business transfers personal data outside of the UK?

Under the current law, in the event that a UK business transfers personal data outside the EEA that business must ensure that there are adequate safeguards in place in respect of that transfer. The safeguards available are as set out in the GDPR and include, for example, putting in place Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), for intra-group transfers. Those safeguards

are not required where an exemption applies or where the European Commission has made an adequacy decision about the country involved.

Following Brexit, the UK GDPR will set out a similar set of rules covering transfers outside the UK. The Brexit Guidance suggests that there are likely to be different rules in place for transfers (i) to the EEA and (ii) to other countries.

In respect of transfers from the UK to the EEA, the Brexit Guidance clarifies that the Government made clear its intention to permit data to flow from the UK to other EEA countries without restriction or requiring additional safeguards. Data can therefore continue to be sent to the EEA without requiring additional measures in place.
In respect of transfers from the UK to other countries, the UK GDPR will contain similar restrictions in respect of that transfer outside the UK to those contained in the GDPR in relation to transfers outside the EEA.

The Brexit Guidance confirms that where a safeguard has previously been put in place under the GDPR in respect of a transfer outside the EEA, those organisations will be able to continue to rely on that mechanism in respect of the transfer outside the UK. Adequacy decisions made by the European Commission before Brexit will be recognised by the UK government going forwards and SCCs and BCRs put in place prior to Brexit will continue to apply. That is certainly helpful for businesses that do not need to put in place additional measures to cover the same transfers after Brexit. However organisations should ensure that they have appropriate transfers in place now, under the current law, as, following Brexit, to the extent both the GDPR and the UK GDPR are applicable, organisations could find themselves in breach of both laws.

In respect of transfers to the US, the Brexit Guidance confirms that although the EU/ US privacy shield will need to be modified, provided certain measures are put in place, organisations can continue to rely on it in the meantime.

What about transfers to the UK from the EEA?

The EU version of the GDPR will also continue to contain restrictions on transfers of personal data outside the EEA. Following Brexit, any transfers from the EEA to the UK will be subject to those restrictions.

The Brexit Guidance clarifies that the EDPB are still finalising guidance on this issue.
UK government has indicated its intention to seek an adequacy decision from the European Commission for the UK. The effect of that would be that any transfers of personal data outside the EEA to the UK would not require an additional safeguard. However, in order for that to be granted, the European Commission will need to recognise the UK's data protection regime as "essentially equivalent" to the EU's.

The process for agreeing adequacy decisions will not begin until the UK has left the EU and there is no telling at this stage how long it will take. As the law will be similar, 'essential equivalence' should in theory be easy to achieve. However any changes in any guidance and case law applicable in the UK after Brexit will inevitably impact on that.
The ICO Brexit guidance is that in the meantime, organisations will need to carefully consider alternative transfer mechanisms, such as SCCs or BCRs, in order to maintain data flows from the EEA to the UK.

What about transfers to the UK from other countries?

To the extent that the UK is receiving personal data from other countries outside the EEA, any applicable restrictions will likely depend on the local law of that country.
However, the Brexit Guidance confirms that Brexit will impact on any transfers to the UK from countries which are subject to an EU adequacy decision which include, Andorra, Argentina, Canada, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay or USA (under Privacy Shield only).

In order to be deemed adequate under that EU adequacy decision, those countries are likely to have their own legal restrictions on making transfers of personal data to countries outside of the EEA. Following Brexit, any transfers from those countries to the UK will therefore be subject to those restrictions.

The Brexit Guidance confirms that it is anticipated that the UK government will enter into discussions with those countries and that further guidance will be made on this issue. In the meantime, organisations receiving data from those countries should seek local advice.

In summary

In summary, although data will continue to be transferable from the UK to the EEA without further safeguards, there will be additional considerations to prepare for and implement in respect of other cross-border transfers of personal data. That will range from seeking local advice (in respect of transfers to the UK from other countries- particularly those subject to an adequacy assessment) to implementing appropriate safeguards (in respect of transfers from the UK to a third country or from the EEA to the UK). We have set out a table at the end of this article summarising the position under the current guidance.

In what circumstances does a UK business need an EU Representative?

The Brexit Guidance also includes guidance around the provisions of the GDPR relating to EU representatives.

The GDPR provides that, subject to certain exceptions, an organisation outside the EEA that (i) offers goods and services within the EEA; or (ii) monitors the behaviour of data subjects within the EEA, must have a representative in the EEA. Following Brexit, that will also apply to organisations in the UK who are subject to the GDPR as a result of its extraterritorial effect.

That representative will need to be set up in the EEA and authorised to act on data protection matters on behalf of the UK business. Practically, that can take a number of forms and the Brexit Guidance suggests that a 'simple service contract' might be the most appropriate in the circumstances.

The Brexit Guidance also clarifies that, following Brexit, the UK GDPR will contain similar provisions, requiring controllers and processors based outside the UK, but to which the UK GDPR is subject, to appoint a UK representative.

Conclusion

There are a number of other practical matters which will be impacted by Brexit. That includes, which supervisory authority will apply for cross-border transfers and documentation, such as privacy policies and records of processing activities, will need to be updated, to deal with the changes to international transfers.

The issues with international transfers, described above will be made considerably simpler if the UK were to receive an adequacy assessment from the EU. However, in order to achieve adequacy, the UK must show that the law in the UK is "essentially equivalent" to the law in the EU. As the GDPR will apply in full (as adapted to refer to the UK) following Brexit, the hope is that "essential equivalence" will be easy to achieve. However, there are ambiguities surrounding a number of areas of the GDPR and the associated guidance of the EDPB and the ICO are important in interpreting those provisions and deciding how it will apply for UK businesses going forwards.

To date, the ICO has placed significant weight on the guidance of the EDPB and has followed the EDPB in its own guidance. However there is a question about whether that will continue to be the case following Brexit, particularly as the ICO will no longer sit on the EDPB and will, potentially, no longer have the ability to influence the guidance that it gives with UK businesses in mind.

Summary of International Transfers

Transfer from	Transfer to	Likely measures to implement based on current guidance
UK	EU	No additional safeguards required.
EU	UK	Safeguards required, in the absence of an adequacy assessment, in accordance with the EU version of the GDPR.
UK	Third country with adequate assessment	No additional safeguards required as the UK will accept the EU's adequacy assessment.
Third country with adequate assessment	UK	Local law may require additional safeguards as a result of the adequacy assessment. Recommend seeking local advice.
UK	Third country without adequate assessment	Safeguards required under UK version of GDPR.
Third country without adequate assessment	UK	Depends on the requirements of local law.

Lauren Webb and Richard Nicholas, Data Protection lawyers at Browne Jacobson LLP

This article was first published in PL&B UK Report, January 2019, www.privacylaws.com.

Contact

Richard Nicholas

Partner

richard.nicholas@brownejacobson.com

+44 (0)121 237 3992

Related expertise

Data protection and privacy