Browne Jacobson

Brexit: data protection law and local authorities?

The political situation in Westminster continues to evolve and it is unclear what will happen on October 31st – in particular whether we will remain, leave, or whether there will be a transitional arrangement to bridge the gap?

18 September 2019

This article is taken from September's public matters newsletter. Click here to view more articles from this issue.

The political situation in Westminster continues to evolve and it is unclear what will happen on October 31st – in particular whether we will remain, leave, or whether there will be a transitional arrangement to bridge the gap? In the event that no-deal does materialise it will not only have an impact on business but also local authorities in a range of spheres.

One of the areas that will be impacted by Brexit is data protection law. Local authorities control and process vast amounts of data for a range of purposes. They do so internally or through the use of contractors and sub-contractors that they appoint to carry out various statutory and non-statutory duties. Some local authorities are likely to have trading companies and those entities will have their own data controlling and processing arrangements in place, which will also be impacted.

So what does Brexit mean for local authorities and compliance with data protection law?

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). In August 2019, the Ministry of Housing, Communities and Local Government (MHCLG) issued guidance to local authorities on accessing data from the European Economic Area (EEA) under a no-deal Brexit (the MHCLG Guidance).

Both sets of guidance will be relevant to all local authorities in England to whom the GDPR currently applies.

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.

The MHCLG adopts a similar approach by strongly encouraging local authorities to conduct a risk assessment and seek legal advice where necessary in relation to processing personal data.

The suggested steps are particularly important, which local authorities should consider in preparing for a no-deal Brexit to ensure that delivery of services is not affected where critical personal data may no longer be accessible after 31st October.

We have summarised in this article the key points relating to the applicable law and cross border data transfers that will have a practical impact for local authorities, as well as the practical steps that local authorities should consider.

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 and the Brexit Guidance makes 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) Act 2018. 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 is a member of and takes into account the guidance of the European Data Protection Board (EDPB), the EU body in charge of the application of the GDPR, when drafting its own guidance and making decisions.

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 local authority or a supplier on its behalf transfers personal data outside of the UK?

Under the current law, in the event that a local authority or a supplier on its behalf transfers personal data outside the EEA (for example a data processing centre in India) the local authority 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 (local authorities or businesses on their behalf) 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 local authorities that do not need to put in place additional measures to cover the same transfers after Brexit.

However local authorities (and any contractors or sub-contractors they engage resulting in data transfers) 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 one set or both sets of laws or they may be required to put in place additional safeguards to enable transfers of personal data.

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. This is unlikely to affect local authorities as generally data is transferring from the UK to another country for processing. However, there is a risk that once data is processed they may not be transferred back without additional safeguards being put in place, which could result in delays.

If the UK cannot get an adequacy decision from the EU it is possible that that the processor could refuse to transfer data back to the local authority unless safeguards are put in place that satisfied the EU version of the GDPR, as continuing without such safeguards may breach that processor’s obligations under the EU version of the GDPR. Alternatively, the local authority will need to use an alternative route set out in the EU GDPR to comply.

What about transfers to the UK from non-EEA countries?

To the extent that the UK is receiving personal data from 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.

Conclusion

Understanding your existing data flows as a local authority, as well as the relationships of the parties engaged in processing personal data as part of your preparations for Brexit is very important. The MHCLG Guidance suggests carrying out a risk assessment and seeking legal advice where necessary to determine your position and the actions that may be required. Whilst the actions that a local authority will need to take will depend on particular circumstances, it is important for local authorities to consider the following:

- reviewing all existing contracts and engaging with existing contractors to determine if:
    - personal data is being processed
    - what are the relationships of the parties
        - controller to controller relationship or controller to processor
    - where is the personal data processed including whether it is being held in different locations such as outside of the UK
- what arrangements are necessary to ensure continuous data flows
- what is required to put those arrangements in place and how quickly can those arrangements be implemented – legal advice may be required to determine as to the arrangements that may be necessary and putting them in place
- identifying critical personal data which affects service delivery and prioritise putting in place the necessary arrangements in respect of those data sets
- consider any other mitigating actions that may be required such as putting in place other arrangements for the short term to continue service delivery
- obtaining sufficient information from prospective contractors as to data arrangements in on-going procurements in order to identify the necessary arrangements that would be required for the longer term.

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.

For more information please contact: Peter Ware, Nat Avdiu or Lauren Webb.

Contact

Mark Hickson

Head of Business Development

onlineteaminbox@brownejacobson.com

+44 (0)370 270 6000

Related expertise

Services

Criminal compliance and regulatory

Data protection and privacy