Client Alert: ICO Brexit and Data Protection Guidance

Date : December 21, 2018

Introduction

In light of a possible no Brexit deal scenario when the UK leaves the EU on 29 March 2019, which looks like a distinct possibility, the UK's data protection regulator, the Information Commissioner's Office (ICO), has issued information and guidance about data protection in this situation.

What's the issue?

Under the EU General Data Protection Regulation (GDPR) organizations can only transfer personal data outside the EU if there is a legal basis for doing so – the bases are very strictly defined. Because such transfers are not restricted within the EU, for the time that the UK remains within the EU there are no data transfer issues as such between the UK and the EU. But, upon exiting the EU the UK will become a "third country" as it will be outside the EU for the purpose of making data transfers, i.e. the GDPR legal criteria for transferring data from outside the EU will apply to the UK. The UK will also have to determine its position as regards data flows from the UK to the EU (and elsewhere) – temporarily at least, data transfers from the UK to the EU should be able to continue uninterrupted.

One existing way under GDPR to make data transfers to countries outside the EU is where the EU has made a so-called "adequacy decision" about a given country – so far this exists for about a dozen countries in the world. The UK hopes that the EU will make such an adequacy decision as regards the UK and is pushing for this to be done sooner rather than later. But, despite the UK's confidence that such an adequacy decision can be eventually made (which is by no means certain), pending any such decision, in a no deal Brexit scenario the legal position governing data transfers from organizations in the EU to organizations in the UK would change. Organizations therefore need to ensure that they will be able to continue to legally transfer data.

What's the ICO's position?

The ICO has published guidance, FAQs and a short "Six Steps to Take" advice document for organisations, which can be found here: https://ico.org.uk/for-organisations/data-protection-and-brexit/. The six recommended steps are as follows:

- Carry on complying – continue to comply with GDPR (and the UK Data Protection Act 2018) and follow ICO guidance;
- EEA (including the EU) to UK data transfers – review data flows and identify where your organisation receives data into the UK from the EEA (including the EU) to ensure sufficient safeguards are in place to allow the continued flow of personal data. Standard contractual clauses/model clauses are the most likely safeguard option for most organisations – multinational organisations should also consider adopting Binding Corporate Rules (BCRs). The ICO has produced an interactive tool about data transfers from the EEA (including the EU) to the UK that takes about 10 minutes to complete, which can be found here: https://ico.org.uk/for-organisations/data-protection-and-brexit/standard-contractual-clauses-for-transfers-from-the-eea-to-the-uk-interactive-tool/;
- UK to EEA (including the EU) data transfers – identify data flows to countries outside of the UK as these will fall under new UK transfer and documentation provisions. The status quo should continue for transfers from the UK to the EEA (including the EU), for now at least; things should also continue as now for UK to non-EEA country data transfers as the UK will likely mirror existing EU adequacy decisions, standard contractual clauses/model clauses and BCRs;
- European operations – for organisations that operate across Europe, data flows, processing operations and group structures should be reviewed to fully understand the effect of Brexit on operations. If the UK is currently your "Lead Supervisory Authority" under the GDPR One-Stop-Shop system you'll need to review the structure of your European operations to assess if you can continue to be able have a lead authority and benefit from the One-Stop-Shop system. If you are based in the UK, and not in any other EU or EEA

state, but you offer goods or services to individuals in the EEA (including the EU), or you monitor the behaviour of individuals located in the EEA (including the EU), then to comply with the EU regime you will need to appoint a suitable representative in the EEA (including the EU). This person will act as your local representative with individuals and data protection authorities in the EEA (including the EU). This is separate from your Data Protection Officer (DPO) obligations, and your representative cannot be your DPO or one of your processors. You do not need to appoint a representative if you are a public authority, or if your processing is only occasional, low-risk, and does not involve special category or criminal offence data on a large scale;
- Documentation – identify privacy documentation in the event it needs to be updated when the UK leaves the EU such as with regard to international data transfers including where Data Protection Impact Assessments are concerned; and,
- Organisational awareness – ensure key people in the organisation are aware of these key issues and that plans are up to date. It would also be useful to review your organisation's risk register, if you have one.

It is worth highlighting the appointment of a data protection representative issue referred to above as many organizations may not have fully come to grips with this yet in general, where it applies to them. GDPR has extra-territorial effect under Article 3(2) of GDPR, i.e. organizations outside the EU are still caught by GDPR in certain defined circumstances. When this applies, Article 27 of GDPR requires a controller or processor not established in the EEA (including the EU) to designate a representative within the EEA (including the EU), but which does not apply to public authorities or if the controller/processor's processing is only occasional, low risk, and does not involve special category or criminal offence data on a large scale. The UK Government intends to legally replicate this provision to require controllers based outside of the UK to appoint a representative in the UK; see the UK's Department for Culture, Media and Sport no-deal Brexit data protection guidance on this here: https://www.gov.uk/government/publications/data-protection-law-eu-exit/amendments-to-uk-data-protection-law-in-the-event-the-uk-leaves-the-eu-without-a-deal-on-29-march-2019.

The UK government has also previously issued technical notices about data transfers between the UK and the EU, which we wrote about here: http://www.corderycompliance.com/uk-brexit-no-deal-notice-and-data-transfers-2/

What are the takeaways?

The takeaway is to have a solid Plan B in case the no deal Brexit scenario occurs, which, to be emphasised again, is a very real possibility. Perhaps the most pressing issue to address is data transfers between the EEA (including the EU), so consider the following:

1. Be proactive – do not leave this until the last-minute and instead approach the organization(s) concerned for discussions about this as soon as you can;
2. Consider which of the relevant GDPR legal bases are possibilities for your organization – standard contractual clauses/model clauses are the most likely candidate because realistically it is very difficult to meet the criteria of the other legal bases or to rely on a derogation;
3. Put in your diary dates for when to action your choices, which would likely best be done by the end of January 2019 at the latest – if you eventually choose standard contractual clauses/model clauses, whilst they can be turned around quite quickly given their nature (but without forgetting that the schedules/appendices to them need to be completed) the logistics of possibly having many sets of agreements to sign off may take some time to complete; and,
4. Once the chosen measures (including standard contractual clauses/model clauses) have been agreed, data protection documentation in the organization would also likely need to be revised to reflect the chosen arrangements.

We report about data protection issues here: http://www.corderycompliance.com/category/data-protection-privacy/

For more about GDPR please also see our GDPR FAQs which can be found here: http://www.corderycompliance.com/eu-data-protection-regulation-faqs-3/ and our Data Protection Glossary which can be found here: http://www.corderycompliance.com/eu-data-protection-glossary/

Cordery's GDPR Navigator includes resources to help deal with data protection compliance. GDPR Navigator includes:

- Detailed guidance on the security aspects of GDPR in paper and on film;
- A template data breach log;
- A template data breach plan; and,
- A template data breach reporting form.
- For more on Navigator please see here: http://www.corderycompliance.com/solutions/cordery-gdpr-navigator/.

See also our short film here on Brexit and Compliance where André Bywater & Jonathan Armstrong discuss how compliance might change post-Brexit. They look at a number of distinct areas of compliance including modern slavery, sanctions and data protection and walk through what businesses might want to do now to make sure they comply.

For more information please contact André Bywater or Jonathan Armstrong who are lawyers with Cordery in London where their focus is on compliance issues.

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com