Brexit — the guidance so far. Keep calm and carry on?

John O'Brien explores key themes emerging from the ICO and UK government on how best to prepare for Brexit

To butcher a catchphrase from a certain wildly popular HBO show: Brexit is coming. Whatever form of Brexit takes place, and whenever it may be, one thing is clear: UK organisations need to prepare themselves.

Previous articles (see for example 'Brexit: key impacts on data protection' by James Clark & Alexandra Greaves, Volume 19 Issue 1, pages 6-8) and commentary in this journal have covered the types of issues that UK organisations will need to consider. Towards the end of 2018, the UK government and regulator began to issue concrete guidance:

- the Information Commissioner's Office ('ICO') issued guidance on the impact of Brexit on UK companies that process personal data; and
- the Department for Digital, Culture, Media & Sport ('DCMS') issued guidance on UK data protection law amendments in the event of a 'no deal' Brexit.

The government has also laid secondary legislation before the Houses of Parliament to amend domestic legislation governing personal data processing, electronic direct marketing and cookies.

Some common themes emerge from the guidance and legislation. This article is a whistle-stop tour of the guidance that UK businesses have received. It is intended to help concentrate minds about what organisations can do now to prepare for Brexit.

The ICO guidance

The overarching message from the ICO is that UK organisations should continue to comply with the General Data Protection Regulation ('GDPR'). Brexit does not mean that the GDPR will disappear from the horizon. The UK government intends to bring the GDPR directly into UK domestic legislation once Brexit takes place.

Organisations will generally be subject to the same data protection requirements after Brexit as they were before Brexit. The ICO also has the following messages for British organisations:

- personal data transfers from the UK to the European Union ('EU') can continue uninterrupted. However, personal data transfers from the EU to the UK will be more difficult (discussed further below);
- if your organisation has an EU-wide Data Protection Officer ('DPO') based in the UK, the ICO wants you to know that Brexit will not majorly impact him/her. The DPO can combine their UK domestic law and EU-wide legal obligations after Brexit. Given there will be limited divergence between UK and EU data protection laws for the foreseeable future, this should not be challenging for UK-based DPOs.

The ICO cannot continue to be an organisation's Lead Supervisory Authority following Brexit, because the regulator will no longer be a member of the European Data Protection Board. This means that organisations will need to assess their EU operations to see whether there is another EU affiliate that can be considered the company's place of central administration in the EU. If yes, the local regulator in that country may become the organisation's Lead Supervisory Authority for the EU and the ICO will remain responsible for regulating UK personal data processing. If not, the organisation may no longer be able to benefit from the GDPR's 'One Stop Shop', with the result that the organisation has to liaise with regulators in each EU Member State they operate in. This could require a significant commitment of resources, both in terms of time and money.

The ICO also stresses the importance that key people in the company should know what is happening. Key decision-makers need to continue to be aware of the importance of complying with the GDPR.

DCMS guidance

Attempting to forecast what kind of Brexit will occur is a fool's game for those of us outside of Westminster or Brussels. Some of the more interesting descriptors include 'negotiated', 'disruptive' and 'disorderly' exits from the EU.

Guidance issued by the DCMS is predicated on the increasingly likely premise

(Continued on page 4)

that the UK exits the EU without a negotiated deal.

In addition to some of the themes of the ICO's guidance, the DCMS's messages for UK organisations are:

- the UK will transitionally recognise all EEA countries (and Gibraltar) as 'adequate' destinations for UK-originated personal data. UK to EEA personal data transfers will not be affected by Brexit;
- the UK will also transitionally recognise existing EU 'Adequacy Decisions' for non-EU countries. This means that UK transfers to countries like Canada, Uruguay and — as of January 2019 — Japan, can continue uninterrupted;
- the UK will recognise 'standard contractual clauses' ('SCCs') in UK law, and empower the ICO to issue new SCCs. This means that UK data exporters can continue to use SCCs as a method for exporting personal data to non-EEA countries that do not have Adequacy Decisions;
- the UK will recognise Binding Corporate Rules that were authorised before the UK leaves the EU. This will no doubt come as a relief to the many organisations that spent a lot of time and effort putting these international data transfer arrangements in place;
- UK data protection law will continue to have extra-territorial scope following Brexit. If an organisation is processing the personal data of individuals located in the UK, it will have to comply with UK data protection law. This is the case even where the company is not established in the UK. This mirrors the extra-territorial effect of the GDPR; and
- non-UK organisations which are subject to UK data protection laws will have to appoint UK-based representatives. This will be required where companies process personal data on a large scale. For example, a global company with a US headquarters will most likely have to appoint its UK affiliate as its US headquarters' UK representative. This is a change that will impact many large companies. Now is the time to start thinking about the appropriate paperwork and corporate authorisations that need to be put in place.

"Given the fractious recent relationship between the UK and EU, it may be wishful thinking to hope that the UK obtains an Adequacy Decision quickly. We must also bear in mind that when granting an Adequacy Decision, the European Commission considers the entire impact of the third country's laws."

UK domestic legislation amendments

Section 3 of the European Union (Withdrawal) Act 2018 allows for the implementation of all direct EU legislation, including the GDPR, into national UK law. However, the UK government needed to make many clarifying amendments so that the GDPR makes sense once it is solely a domestic piece of UK legislation.

The UK government has attempted to address this by publishing the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 ('2019 Regulations'). The 2019 Regulations purport to maintain data protection standards that currently exist in the UK under the GDPR and Data Protection Act 2018. It converts EU-wide obligations to UK-only obligations. Existing references to EU Member States, institutions, procedures and decisions, will no longer be directly relevant after Brexit. These references have been replaced with references to their UK domestic equivalents.

Additionally, the 2019 Regulations legislate for the various issues set out in DCMS's guidance. For example, they retain the concept of extra-territorial application, and introduce the obligation for non-UK controllers to designate UK representatives in certain circumstances.

The elephant in the room

Continued personal data transfers from the EU to the UK remain the elephant in the room. This is not an issue that the UK government can unilaterally solve. The ball remains firmly in the EU's court.

The problem is that, after Brexit, the UK is a non-EU third country. It does not have an Adequacy Decision from the European Commission. It does not have a special international transfer arrangement like Privacy Shield for the USA.

The Political Declaration on the future EU-UK relationship, published alongside the draft Withdrawal Agreement between the EU and UK, specifically addressed this issue. It stated that the European Commission would endeavour to grant the UK an Adequacy Decision by the end of 2020. However, at the time of writing, it looks increasingly unlikely that the UK will agree to the Withdrawal Agreement.

In the event of a 'no deal' Brexit, organisations will need to change how they make international data transfers. It is likely that many large organisations will already have detailed intragroup data transfer agreements in place. It is also likely that such agreements will be modelled on SCCs, with EEA data exporters and non-EEA data importers. One (relatively) low stress solution could be to amend these agreements and include UK entities as non-EEA data importers.

Organisations need to understand how personal data flows within their

organisation. This should be a lot easier now for those organisations that undertook extensive GDPR preparation projects.

There are fewer immediate solutions for personal data transfers that involve suppliers, vendors or other third parties. Existing contracts with such third parties will need to be updated to facilitate the export of EEA personal data to the UK.

It remains to be seen whether there is sufficient appetite within the European Commission to issue the UK with an Adequacy Decision. Such decisions usually take at least two years to negotiate, and this is where there is goodwill on both sides. Given the fractious recent relationship between the UK and EU, it may be wishful thinking to hope that the UK obtains an Adequacy Decision quickly.

We must also bear in mind that when granting an Adequacy Decision, the European Commission considers the entire impact of the third country's laws. The EU is uncomfortable with the degree of latitude that the UK's security services have to monitor and intercept personal data for national security purposes. This could prove to be a major stumbling block to the granting of an Adequacy Decision to the UK.

Conclusion

The ICO and DCMS guidance is helpful. It clarifies many issues that organisations are worried about. The 2019 Regulations also show that the UK government knows that data protection is a key Brexit concern for businesses.

Very few businesses with UK operations are enjoying the uncertainty that Brexit has created. As we hurtle towards 29th March 2019, businesses need to do what they can to ensure they can maintain their UK operations. This requires a close look at their operations in light of the guidance set out in this article. Unfortunately, as has become increasingly clear with all things Brexit-related, quick fixes will be few and far between.

John O'Brien
Reed Smith LLP
jobrien@reedsmith.com