Introduction

This article is aimed to provide guidance to UK businesses and organisations on how Brexit might affect their data protection operations and will be of particular relevance to UK businesses and organisations which:

- send personal data outside of the UK;
- receive personal data from the European Economic Area (the "EEA"); and / or
- operate within the EEA.

We advise that you take this time now, prior to the UK’s departure from the EU, to consider your organisation’s data flows between the UK and the EEA (such as any vendor / customer contracts) and how these might be impacted by Brexit.

Data Protection Legal Framework in the UK Post-Brexit

UK GDPR:

The EU (Withdrawal) Act 2018 (the “Withdrawal Act”) sets out which existing EU law should be kept as UK domestic law after the UK leaves the EU. If the UK leaves the EU under a No-Deal Brexit, then, in accordance with section 3 of the Withdrawal Act, the EU's General Data Protection Regulation (the “EU GDPR”) will become 'retained EU law' and form part of UK domestic law on 29 March 2019 (the "UK GDPR"). As a result, the EU GDPR (or rather a revised version of it) will continue to apply in the UK.

Since the UK will no longer be an EU Member State, and the EU GDPR refers to EU laws and institutions, the EU GDPR will need to be modified in order to make sense in the UK post-Brexit. The draft 'Data Protection, Privacy and Electronic Communications (Amendments etc) (EU exit) Regulations 2019' (the "Exit Regulations") provide the statutory instrument through which these modifications would be made.

The Exit Regulations contain provisions to:

- maintain the EU GDPR standards in UK domestic law;
- enable flows of personal data from the UK to the EEA by initially recognising all EEA / EU countries (and Gibraltar) as ‘adequate’;
- maintain the extraterritorial scope of the UK data protection framework;
- require all non-UK organisations who are subject to the UK GDPR to appoint data protection representatives in the UK (if they are processing the personal data of individuals in the UK on a large scale);
- recognise all existing adequacy decisions made by the EU (subject to ongoing review);
recognise EU Standard Contractual Clauses (“SCCs”) in UK law and give the ICO the power to issue new clauses; and
recognise Binding Corporate Rules (“BCRs”) authorised prior to the UK’s exit from the EU and give the ICO the power to approve new BCRs.

The Data Protection Act 2018 (“DPA”):
The DPA is UK law and will therefore continue to apply to the use of personal data in the UK after the UK’s departure from the EU.

PECR / e-Privacy Regulation:
It has been confirmed by the UK Government that, upon the UK’s exit from the EU, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (“PECR”) will continue to apply in the UK.

To the extent that the EU’s proposed e-Privacy Regulation (once finalised) is not incorporated into UK law and that the e-Privacy Regulation differs from PECR, organisations may need to comply with dual regimes under UK and EU law in relation to direct marketing to individuals in the UK and the EEA and the other requirements associated with electronic communications set out in PECR and the e-Privacy Regulation.

Key Considerations for Organisations in Relation to a No-Deal Brexit

Given the immediate impact that a No-Deal Brexit would have on organisations with a UK presence, we would advise that such organisations consider the following key questions on how a No-Deal Brexit is likely to affect their data processing operations:

“Which data protection laws will apply to my organisation in the event of a No-Deal Brexit?”

Territorial Scope

Although the provisions set out under the EU GDPR and UK GDPR would be very similar, the two laws should be seen as distinct. It is therefore important that your organisation is aware of which law(s) govern(s) their data protection procedures.

- **EU GDPR**: Following the UK’s departure from the EU, organisations established in the UK (and with no establishment in the EU) will only be subject to the EU GDPR to the extent that they are processing personal data of individuals in the EEA and to the extent that such processing activities are related to the offering of goods or services of such individuals, or the monitoring of their behaviour.

  The territorial scope of the EU GDPR in relation to those organisations established outside the UK will not be changed as a result of Brexit.

- **UK GDPR**: Under the Exit Regulations, the UK GDPR will have a territorial scope which mirrors that of the EU GDPR, such that the UK GDPR will apply to organisations which are either established in the UK or outside of the UK if they process the personal data of the individuals in the UK in the context of offering them goods or services or monitoring their behaviour.

- **DPA**: The DPA has the same territorial scope as the UK GDPR (see above).

There is therefore a strong possibility of dual regulation for multi-national organisations. For example, organisations in the EEA might be subject to the UK GDPR (as well as the EU GDPR and the DPA), whilst organisations in the UK might still be subject to the EU GDPR (as well as the UK GDPR and the DPA).
“Who will be my organisation’s data protection supervisory authority in the event of a No-Deal Brexit?”

Supervisory Authorities

After the UK leaves the EU, the UK Information Commissioner’s Office (the “ICO”) will continue to operate as the UK’s independent supervisory authority on data protection. The ICO will also supervise the activities of organisations outside of the UK to the extent that they are subject to the UK GDPR.

Additionally, organisations who operate in the UK may also be subject to the EU GDPR and therefore the supervision of the applicable data protection authority in the EU.

This could mean that an entity may be supervised and potentially fined by an EU data protection authority as well as the ICO.

Lead Regulators

Once the UK leaves the EU, the ICO will no longer be able to act as a lead authority in respect of breaches of the EU GDPR. As a result, a data protection authority in the EU will act as the lead authority in respect of breaches of the EU GDPR and there may well be no formal requirement for the EU data protection authorities to collaborate and co-ordinate with the ICO (although informal collaboration and co-ordination seems likely).

“Will my organisation need to appoint any additional data protection representatives in the event of a No-Deal Brexit?”

Representatives

Under the EU GDPR, a controller or processor not established in the EEA who processes personal data in scope of the EU GDPR must designate a data protection representative within the EEA. The requirement 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 replicate this provision in the UK GDPR, requiring organisations which are based outside of the UK to appoint a representative in the UK where they are subject to the UK GDPR.

In the event of a No-Deal Brexit, EEA and UK organisations may therefore need to appoint:

- a data protection representative in the EEA if their EEA data protection representative is currently located in the UK; and / or
- a data protection representative in the UK if they are based outside the UK but are subject to the UK GDPR.

“How would a No-Deal Brexit affect how my UK organisation processes personal data within the UK?”

Even in the event of a No-Deal Brexit, the DPA will continue to operate in the UK and will sit alongside the UK GDPR, and should maintain equivalent data protection standards in the UK. There should therefore be no immediate changes to the UK’s own internal data protection standards and those standards are currently very similar to those applicable in EEA countries.

“Will my UK based organisation be able to continue to transfer personal data outside of the UK into the EEA in the event of a No-Deal Brexit?”

The Exit Regulations maintain in the UK GDPR the same restriction for data transfers outside of the UK as the restriction which exists in relation to the EU under the EU GDPR. This restriction under the UK GDPR would apply to all non-UK countries (including those countries in the EEA).
However, given the level of alignment between the UK’s and the EU’s data protection regimes, the UK Government has stated that all remaining EU / EEA countries (and Gibraltar) together with all non-EEA countries which have already been granted adequacy status by the EU Commission will be granted adequacy status by the ICO. It should be noted, though, that this position will remain under constant review. Additionally, under the Exit Regulations, the UK’s ICO will be able to make adequacy decisions in relation to other countries.

Under the Exit Regulations, the UK will also continue to treat those US entities which are self-certified under the EU-US Privacy Shield mechanism in the same way.

This will mean that, if the UK leaves the EU under a No-Deal Brexit on 29 March 2019, transfers of personal data from the UK to the EEA will continue to be unrestricted under UK law.

“How would a No-Deal Brexit affect my UK based organisation’s transfers of personal data to organisations outside of the EEA?”

The same restrictions as under the EU GDPR in relation to transfers of personal data outside of the EEA will continue to apply under the UK GDPR. If your organisation is already transferring personal data outside of the EEA, then it should already have arrangements in place for making these restricted transfers – e.g. SCCs and BCRs.

Importantly, the UK will continue to recognise BCRs and SCCs as adequate data transfer solutions to such entities and those BCRs and SCCs which have previously been certified by the ICO and EU will continue to be recognised by the UK after the UK’s departure from the EU.

Under the Exit Regulations, the ICO will, on the UK’s exit from the EU, have the power to issue new BCRs and SCCs. SCCs and BCRs may therefore continue to be used as possible mechanisms to enable transfers of personal data outside of the UK (either in their current form or modified by the ICO).

“How would a No-Deal Brexit affect my UK based organisation’s ability to receive personal data from the EEA?”

Under the EU GDPR, transfers of personal data from the EEA to outside of the EEA (to a “third country”) are “restricted transfers” and are only allowed under the EU GDPR to the extent that the receiving country has an adequacy decision, an appropriate safeguard (e.g. SCCs or BCRs) is in place or if a relevant exemption can be relied upon.

If there is a Deal Brexit (i.e. the UK and the EU approve the draft Withdrawal Agreement which is currently before the UK Parliament), then the UK will essentially continue to be dealt with by the EU as if it were still part of the EU. This would mean that the UK shall not, transitionally, be treated as a third country by the EU, and there will therefore be a free flow of personal data between the UK and the EEA until the end of the transition period (i.e. until, at the earliest, 31 December 2020).

However, if the UK leaves the EU with a No Deal Brexit, the UK will be treated as a third country by the EU and will be subject to data transfer restrictions under the EU GDPR. Accordingly, EEA based controllers and processors will need to ensure that they have appropriate data transfer solutions in place to cover EEA-UK data transfers.

The European Commission has suggested that it would make an adequacy decision in relation to the UK if it deems the UK to provide an adequate level of protection for personal data. This would enable the free flow of personal data from the EEA to the UK. However, the European Commission has yet to indicate a timetable for this and has made it clear that such discussions will not take place until the UK has left the EU (and actually become a third country). Whilst the decision ought to be relatively straightforward (given that the UK’s laws are closer to the EU GDPR than any other country given adequacy status by the EU) adequacy determinations can take some time to finalise and there will inevitably be a period of time in which the UK is regarded as a third country.

UK based organisations receiving personal data from the EEA should therefore put in place measures to make the transfer of data from the EEA to the UK compliant with the EU GDPR. For the majority of organisations and transfers, this will be achieved through the use of SCCs, although in some situations, it may be possible to rely upon a derogation to transfer the personal data.
We note that the European Commission has not currently issued SCCs in relation to transfers of personal data from EEA data processors to data controllers outside of the EEA. Arguably, to the extent that the transfer is simply the return transfer of personal data by the EEA data processor to the non-EEA data controller, such a data transfer would not be governed by the EU GDPR. Ultimately, however, the extent to which such transfers would be governed by the EU GDPR depends on the views of the relevant EU data protection supervisory authority in which the EEA data processor is located and Simmons & Simmons is currently in the process of collating the views of the data protection supervisory authorities across the EEA on this matter. In some instances, it appears that the position is not yet clear.

“Will I be subject to the same fines in relation to any data protection breaches in the event of a No-Deal Brexit?”

Under the Exit Regulations, the ICO will be able to administer the same levels of fine under the UK GDPR as under the EU GDPR.

Simmons & Simmons LLP