Cybersecurity, Data Privacy & Information Management
Alert

Weil

February 4, 2019

Data Privacy - Brexit Considerations – What if there is a "no deal" ?

By Barry Fishley

In this note we consider the implications if the United Kingdom leaves the European Union without agreement of the draft withdrawal agreement. Given the House of Commons' rejection of the draft withdrawal agreement on 15 January 2019, organisations need to ensure they are prepared for a no-deal Brexit scenario.

The draft withdrawal agreement provides that during a transition period ending on 31 December 2020, EU law, including the General Data Protection Regulation ("**GDPR"**), will continue to apply to the UK and references to a "Member State" in the GDPR will include the UK. In the event of a no-deal Brexit, the UK will exit the EU on 29 March 2019 and there will be no transition period.

Current Legal Framework

The Data Protection Act 2018 is an Act of the UK Parliament, which applies the same requirements and standards as the GDPR and is read alongside the GDPR. It will continue in force until it is amended or repealed. Additionally, the EU (Withdrawal) Act 2018 is legislation which will retain all existing directly applicable EU law, including the GDPR, into UK law at the end of the transition period, or if there is no Brexit deal, on the exit date of 29 March 2019. The draft Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (the "**Draft Regulations**") creates the 'UK GDPR,' which will be a single data protection regime within the UK, merging the GDPR and the Data Protection Act 2018. The Draft Regulations are expected to come into force on the exit date or the end of the transition period, if applicable. Therefore, the data protection standards in the UK will remain the same after Brexit, and if a deal is agreed, the GDPR and the Data Protection Act 2018 will continue to co-exist during the transition period as they do presently. While the data protection regimes of the UK and the EU will likely initially have the same standards, the two regimes may diverge over time as further changes to the EU data protection regime made after the exit date or end of the transition period will not be automatically included in the UK regime and vice versa.

International Transfers of Personal Data

Under the GDPR, there is a general prohibition on transfers of personal data outside of the EEA. Personal data can only be transferred to a third country outside of the EEA if the receiving country is deemed by the European Commission to offer an adequate level of data protection,

appropriate safeguards are in place or a derogation applies, such as explicit consent. After a no-deal Brexit or at the end of the transition period, the UK will be a third country for these purposes.

The UK Parliament has confirmed its intention to demonstrate that the UK provides an adequate level of data protection. While it is likely that the UK will be deemed an adequate jurisdiction due to the standards in the Data Protection Act 2018, an adequacy decision is not automatic and the timetable for a decision being made is difficult to predict. Additionally, the European Commission has indicated that the adequacy assessment process will only begin once the UK has withdrawn from the EU. Accordingly, there will probably not be an adequacy decision in place by the exit date in a no-deal scenario and the UK might not be deemed to offer an adequate level of data protection by the end of the transition period under a withdrawal agreement.

Without the UK being deemed to offer an adequate level of data protection, personal data could still be transferred from within the EEA to the UK using appropriate safeguards, such as Binding Corporate Rules or standard contractual clauses, or by using a derogation such as the explicit consent of the individuals.

Under the Draft Regulations, all EEA countries and all countries recognised as offering adequate protection by the EU Commission prior to the exit date would be recognised as offering adequate protection for the purposes of data transfers from the UK on a provisional basis, and no additional safeguards would be required after Brexit for a UK organisation to transfer personal data to these countries. Additionally, the Draft Regulations would provisionally recognise the EU Commission's standard contractual clauses and the Binding Corporate Rules authorised prior to the exit date under UK law. As a consequence, there would be little immediate impact on UK organisations transferring personal data outside of the UK.

After the exit date or the transitional period, if applicable, a US organisation may continue to use the EU-US Privacy Shield Framework to receive personal data from the UK. To do so, the US organisation must maintain a current Privacy Shield certification and explicitly state in its public commitment and its HR privacy policy, if applicable, that its commitment to comply with the Privacy Shield applies to personal data received from the UK.

Supervisory Authorities

Under the GDPR, an organisation carrying out cross-border processing activities in the EEA may benefit from the 'one-stop-shop regime, under which the organisation only has to deal with one supervisory authority in respect of the cross-border processing. An organisation carrying out cross-border processing in the UK and EEA member states will, after the exit date or transition period, have to deal with both the ICO and the EEA lead supervisory authority.

Representatives

After Brexit, organisations that are based in the UK, but that are subject to the EU data protection regime because they offer goods or services to individuals in the EEA or monitor the behaviour of individuals in the EEA, may be required to appoint a representative within the EEA if they do not have an EEA presence. Additionally, controllers based outside of the UK, but that are subject to the UK data protection regime, may be required to appoint a representative within the UK.

Key Takeaways:

- The same data protection standards will continue to apply in the UK after Brexit.
- It is unlikely that the UK will be deemed to offer an adequate level of data protection by the exit date and an adequacy decision might not be made by the end of any transition period. After the end of the transition period or after the exit date if there is no deal, in the absence of an adequacy decision, organisations will need to implement adequate safeguards such as standard contractual clauses or Binding Corporate Rules to lawfully transfer personal data from the EEA to the UK. To prepare for a potential no-deal Brexit, organisations that transfer personal data from the EEA to the UK should implement such safeguards prior to 29 March 2019.

- There will be little immediate impact on UK organisations transferring personal data outside of the UK, including to the EEA, provided that the current lawful grounds for the transfer are adopted.
- Organisations carrying out cross-border processing in the EEA and the UK will no longer be able to use a single lead supervisory authority.
- Organisations should assess whether they will be subject to the UK and EU data protection regimes and whether they will need to appoint a representative in the UK or the EEA.

If you would like more information about the topics raised in this briefing, please speak to your regular contact at Weil or to any member of the Cybersecurity, Data Privacy & Information Management Group.

Barry Fishley View Bio barry.fishley@weil.com +44 20 7903 1410