Countdown to Brexit Series

What should you be doing now?

The fifth in our series of Countdown to Brexit - Data transfers

WALKER MORRIS

Introduction

Cross-border data flows and the openness of the digital economy are essential to the UK's trading relationships with the EU, the US and the rest of the world. All the while that the UK has been a part of the EU, businesses have come to rely on the seamless flow of personal data in their dealings with customers and suppliers. As the UK prepares to leave the EU, with or without a deal, we set out the latest position on transfers of personal data from and to the UK, and the protective steps businesses and other organisations should take now to ensure compliance.

Deal or no deal?

If the UK leaves with a deal, the current rules are generally expected to continue to apply during any transition period. Businesses and organisations should nevertheless plan ahead in light of the uncertainties surrounding data transfers once that period comes to an end.

What about GDPR?

The EU General Data Protection Regulation (**GDPR**) is not going away and will remain important. The UK is committed to maintaining high data protection standards post-Brexit. A UK version of GDPR will ultimately be absorbed into UK law. Essentially, businesses and organisations will still need to comply with the same core data protection principles as they do now. If GDPR currently applies to your processing of personal data this note will be relevant for you. It will not be relevant if you only transfer personal data outside the UK to consumers or only receive personal data from outside the UK directly from consumers, as neither of these are 'restricted' transfers under GDPR.

Data transfers from the UK

In the event of no deal, the UK government has confirmed that UK businesses and organisations will continue to be able to legally send personal data from the UK to the European Economic Area (**EEA**) and there is no need to take preparatory action. It also intends to recognise the European Commission's 'adequacy decisions' made to date (see below), which means that transfers can continue from the UK to those countries or territories. Transfers *from* those countries or territories to the UK will be subject to local law requirements. Modified arrangements will apply in relation to transfers from the UK to the US (see below). In relation to transfers from the UK to any other jurisdiction, consideration will need to be given to available alternative data transfer mechanisms (unless one of a number of limited exceptions applies). These are discussed below. If such transfers are already being made now, GDPR compliance should already have been considered.

Data transfers from the EEA to the UK

Transfers from the EEA to the UK will be affected by Brexit, because (as things stand) the UK will no longer be a part of the EEA and will become a 'third country' for the purposes of data protection law in the event of no deal or once any transition period has expired.

Personal data must only be transferred out of the EEA if it is being transferred to a country which ensures an adequate level of protection for that data. The European Commission may find that a country ensures such an adequate level of protection by reason of its domestic law or the international commitments it has entered into in order to protect individuals' rights.

A Commission adequacy decision for the UK is widely seen as the key to ensuring the continued free flow of personal data from the EEA to the UK. To date the Commission has recognised 13 countries or territories as providing adequate protection (including the USA and Canada, which are subject to partial adequacy arrangements). Any adequacy assessment will not commence until the UK has left the EU. If the UK leaves with a deal, the assessment is expected to take place during any transition period.

The UK obtaining an adequacy decision is by no means a foregone conclusion. There may be concerns in Europe over issues such as the compatibility of the UK's national security and surveillance practices with EU law and the fact that the UK has decided not to retain the EU Charter of Fundamental Rights. There is also no guarantee that any adequacy decision will not be revoked in the future or ruled invalid by the Court of Justice of the European Union. Finally, adequacy assessments take time. Even where there is a transition period, it may not be possible to achieve an adequacy decision within that timescale, although that will depend to a certain extent on whether such a period is ultimately extended.

In the absence of an adequacy decision in respect of the UK (either in the event of no deal or if a decision has not been issued prior to the end of any transition period), EEA controllers and processors will need to consider alternative data transfer mechanisms (unless one of a number of limited exceptions applies).

Alternative data transfer mechanisms and other 'appropriate safeguards'

A key alternative data transfer mechanism for most businesses is the use of standard contractual clauses. These are standard templates which have been adopted by the European Commission for use between controller and controller and controller and processor and the UK government intends to recognise them. The UK's data protection regulator, the Information Commissioner's Office (**ICO**), has produced template contracts containing explanatory notes and guidance: see this link.

Where transfers are being made within a multinational group, from EEA based controllers or processors to non-EEA based controllers or processors, the use of binding corporate rules is another option. The UK government intends to recognise binding corporate rules authorised before the date of exit, covering the UK sender of data and the receiver wherever they are located. EEA binding corporate rules will need to be updated so that the UK is listed as a third country outside the EEA. The European Data Protection Board has published a no deal Brexit note on binding corporate rules for companies which have the ICO as their 'lead supervisory authority'.

Other appropriate safeguards include legally binding and enforceable arrangements between public authorities or bodies.

Data transfers to the US and the EU-US Privacy Shield

The European Commission's adequacy decision for the US concerns personal data transfers covered by the EU-US Privacy Shield certification framework, which US companies sign up to. If the UK leaves the EU without a deal, personal data can continue to be transferred from the UK to US organisations participating in the Privacy Shield, where the participating organisation's privacy policy includes personal data transferred from the UK in its Privacy Shield commitments. UK companies will need to ensure that their US counterparts have made the necessary changes. See the Privacy Shield and the UK FAQs section of the official Privacy Shield website.

Note: *The validity of the Privacy Shield and the Commission's standard contractual clauses are both currently subject to legal challenges in Europe. Walker Morris will continue to monitor and report on developments.*

Other issues

UK based controllers or processors with no office, branch or other establishment in the EEA, but who offer goods or services to EEA individuals or monitor their behaviour, will still need to comply with the EU version of GDPR in the event of no deal. In some cases this will include the requirement to appoint a representative in the EEA: see the ICO guidance.

The GDPR's 'one-stop-shop' mechanism generally allows controllers and processors inside the EEA which carry out processing that affects individuals in more than one EU or EEA state to be regulated by one data protection authority, preventing multiple fines being issued for the same breach. The ICO will no longer participate in this mechanism and it has published detailed guidance for UK based controllers or processors currently carrying out cross-border processing of personal data within the EEA in a number of different scenarios.

What should you be doing now?

- Continue to comply with GDPR standards.
- Review your incoming and outgoing international personal data flows and ensure that you understand how, and via which mechanism, personal data is currently transferred across borders.
- If you receive personal data from the EEA, consider how you can continue to receive that data lawfully if there is no adequacy decision in place for the UK, either in the event of no deal or further down the line if there is a transition period. Keep in mind that setting up alternative data transfer mechanisms is likely to take time and come with associated cost and administrative burdens. You may need to prioritise certain transfers.
- Even if the UK leaves with a deal, the uncertainty surrounding the exact content of that deal and the ICO's role during any transition period as a 'lead supervisory authority' and as part of the 'one-stop-shop' mechanism, means it would be prudent to consider now your position in respect of any binding corporate rules and to review the structure and activities of any European operations to assess what action may need to be taken.
- Review and be prepared to update privacy information and other documentation, including agreements which may contain restrictions on the transfer of personal data. This ICO guidance is a good starting point.

Contact

Jeanette Burgess, Partner
Regulatory & Compliance
+44 (0)113 283 2632
jeanette.burgess@walkermorris.co.uk

Andrew Northage, Partner
Regulatory & Compliance
+44 (0)113 283 4543
andrew.northage@walkermorris.co.uk

WALKER MORRIS