October 2018

Brexit, your business and data: personal data transfers

As the UK government perseveres with the unenviable task of negotiating the UK's exit from the European Union (EU), UK businesses are understandably becoming increasingly wary of the uncertainty that remains around their future operations with regard to the use of personal data. With B(rexit)-Day looming closer, the government has released a series of guidance notes intended to help prepare the public for a 'no deal' situation.

Although the recent notice in relation to data protection is comforting in some respects, it also raises further issues, namely:

- how transfers of personal data between the UK and the EU will be regulated post Brexit;
- that UK businesses operating within the EU will need to adjust to having a new regulator; and
- that UK businesses dealing with EU citizens and their personal data will need to appoint a representative in the EU.

This briefing is the first of two in which we analyse the government's guidance and explore the implications of a 'no deal' Brexit for UK businesses and data, as well as highlighting other important data protection considerations and suggested solutions to prepare for Brexit, regardless of the deal struck.

In this briefing, we consider the impact of a 'no deal' on data flows in and out of the UK - arguably the issue with the greatest consequence. In particular we look at data flows from the EEA to the UK (whilst the guidance note issued by the government only refers to the EU, we must assume that it will also catch data from other EEA countries by virtue of their adoption of the General Data Protection Regulation (2016/679) (GDPR). It is less clear whether data transferred to EEA countries is caught by the guidance note, which doesn't seem to clearly address the issue.)

Will the UK's data protection standard change?

Not really. The EU Withdrawal Act will incorporate the GDPR into UK law and the Data Protection Act 2018 will continue to sit alongside it, so, reassuringly, the time and money invested in becoming GDPR compliant will not be wasted.

Although on the face of it the legal backdrop will not materially change, difficulties arise when considering the implications of the imminent status change of the UK when it ceases to be a Member State, in particular in relation to continued data flows.

UK data flows to the EU

The government has stated that it will permit transfers of personal data from the UK to those

Member States remaining in the EU. In theory, this should mean that no further action is necessary in order to send personal data to EU-based third parties. As a matter of good practice however, it will be worth keeping an eye on any changes to domestic laws of the relevant Member States in the event that new laws create further hoops for the UK to jump through in the future.

EEA data flows to the UK

Transfers of personal data from the EEA into the UK are not as simple. From 29 March 2019, in the event of a 'no deal', the UK will automatically become a "third country" (i.e. a country outside the EEA). At this point, businesses which transfer personal data from the EEA to the UK will need to find a GDPR compliant mechanism in order to continue doing so.

The government doesn't appear to be particularly concerned with this predicament, as it seems to be hedging its bets that the Commission will soon declare such transfers lawful on the basis of an adequacy decision (a decision that the UK has an adequate level of data protection to ensure the safety of personal data outside the EEA). It is easy to see why it would be logical for the Commission to arrive at this conclusion - the theory being that our domestic data protection law will not have changed and the GDPR will still take effect in the UK by virtue of the implementing legislation. In fact, in comparison to the current 12 countries who have benefited from an adequacy decision thus far, the UK stands in a favourable position as traditionally it has been one of the Member States which to date has adopted a high standard when it comes to implementing European data protection laws. In addition, the UK has one of the most sophisticated and influential data protection regulators in the EU and a long history of operating in line with the Commission's approach with regards to the safety of personal data.

However, upon closer inspection, there are a few flies in the adequacy ointment.

- Firstly, the Commission can only make an adequacy decision in relation to a third country, but the UK will not become one until 29 March 2019. Arguably, the Commission could begin preparations now in anticipation of Brexit (deal or no deal) but it would appear otherwise preoccupied with current negotiations.
- Secondly, adequacy decisions have historically not been particularly forthcoming. Adopting an adequacy decision involves a multi-stage procedure including obtaining the approval of the remainder of the EU, which is likely to be time consuming. Depending on the manner of the UK's exit, it is also possible that Member States may be reluctant to agree to this solution, which would further prolong the process.
- Finally, adequacy decisions are not indefinite. These decisions are subject to ongoing review and therefore are capable of being withdrawn at any time, which would bring UK businesses back to square one regarding their ability to process data from the EEA.

What can businesses do?

Whilst the UK awaits its adequacy decision, the GDPR provides for a seemingly more straightforward solution: contractual "model clauses".

Many UK businesses are already familiar with Commission approved model clauses: standard contractual clauses drafted by the Commission which controllers can use as a mechanism to ensure the safety of personal data being sent outside of the EEA, by requiring the recipient of the data (whether a controller or processor) to adopt these clauses. Many businesses have done this as part of their GDPR compliance programme, for example where an EU based company uses a US entity for data hosting facilities. For now, model clauses seem to be the most practical solution for businesses that rely on the in-flow of personal data from the EEA.

Are there any other options?

It may be possible for businesses to rely on the derogations set out in the GDPR for specific situations which allow for the transfer of data from the EEA to a third country in the absence of an adequacy decision, model clauses or binding corporate rules (a complex mechanism which could provide a solution for some corporate groups but would need a longer period to implement before B(rexit)-Day). Examples include explicit consent, contractual necessity and cases relating to legal claims. However, use of these derogations was intended to be limited hence only being permitted if they are used in specific situations and if certain conditions are satisfied. For example, not only will explicit consent need to be GDPR compliant, but the information made known to the data subject must include the possible risks of the transfer.

Moreover, many of the derogations under Article 49 - including the contractual necessity and legal claim derogations - can only be used occasionally and when necessary ("requiring a close and substantial connection between the data transfer and the purposes of the contract"). This means that in practice, whilst the derogations could be useful for occasional transfers in particular circumstances, they are unlikely to be an effective solution in the long term.

Clearly there are a number of factors to consider when evaluating the future ability to transfer data from the EEA into the UK, regardless of the outcome of the current Brexit negotiations. Whilst a lot of us will be keeping our fingers crossed for a speedy adequacy decision, it would be prudent to analyse the data transfers into the UK in respect of your business and their current legal basis to identify the data flows at risk post-Brexit. Businesses should also review their existing contracts for clauses with absolute prohibitions on transferring personal data outside the EEA.

Next steps:

The most sensible option to ensure you are able to continue receiving data from the EEA seems to be the implementation of model clauses by 29 March 2019. Adopting model clauses is a relatively quick and easy process but the first step will be to invest time sooner rather than later to:

- pinpoint your material data transfers;
- work out the data flows; and
- identify with whom you might need model clauses to govern the transfer.

Once you've undertaken the analysis above, the implementation of the model clauses could be postponed until the start of next year, in case of further developments.

Ultimately, everyone will be waiting to see the lay of the land following the Brexit negotiations. There has been some suggestion that contingency plans drawn up by Brussels for a 'no deal' scenario, may well provide some limited relief to secure data flows in from the EEA. However as yet no detail has been provided, and much depends on how talks progress at the summit of EU leaders which commences on 17 October 2018.

In the next briefing, we will be looking at the effect of the UK becoming a third country from an administrative standpoint and in particular, the impact of new regulators and the requirement for many businesses to appoint a representative in the EU.

FOR FURTHER INFORMATION, PLEASE CONTACT

10 Snow Hill
London EC1A 2AL
T: +44 (0)20 7295 3000
F: +44 (0)20 7295 3500
www.traverssmith.com

Dan Reavill
Head of Commercial, IP & Technology

E: dan.reavill@traverssmith.com
T: +44 (0)20 7295 3260

Louisa Chambers
Partner, Commercial, IP & Technology

E: louisa.chambers@traverssmith.com
T: +44 (0)20 7295 3344

James Longster
Partner, Commercial, IP & Technology

E: james.longster@traverssmith.com
T: +44 (0)20 7295 3496

Anita Sivapalan
Associate, Commercial, IP & Technology

E: anita.sivapalan @traverssmith.com
T: +44 (0)20 7295 3720