SLAUGHTER AND MAY/

Beyond adequacy - Brexit's wider data privacy implications

Beyond Brexit – Part of the Horizon Scanning series

A version of this article first appeared in the Privacy Laws & Business UK Report, Issue 110 (July 2020)

Brexit planning should now firmly be on everyone's agendas as the end of the transition period looms closer.

From a data privacy perspective, much of the attention to date has focused on the likelihood of an adequacy decision to enable the free flow of data between the EEA and the UK, with the CJEU decision in Schrems II reducing the odds of this happening even further. Whilst adequacy and international transfers are important considerations given the amount of personal data that currently flows freely, there are other Brexit-related data privacy issues that have received less attention which also need to be addressed. A number of these are considered below.

Application of EU and/or UK GDPR

The UK has a long history of strong data protection legislation and this looks set to continue with the EU General Data Protection Regulation ('EU GDPR') to be written into UK law at the end of the transition period, effectively creating a UK GDPR.

After the transition period, some businesses will become subject to both the EU and UK GDPR because:

- Some will have establishments in both the EU and the UK;
- Others will be caught by the extra-territorial provisions of the EU or UK GDPR where they offer goods or services to individuals in the EU/UK or monitor their behaviour in the EU/UK; and
- Finally, as a result of the EU-UK Withdrawal Agreement, some UK businesses will have to comply with the EU GDPR in relation to a subset of their data (including, in particular, data which relates to individuals in the EU that was processed in the UK during the transition period).

Businesses therefore need to assess which regime applies, and to which data, so that they fully understand their obligations.

Whilst the EU and UK GDPR are near-identical now, there is the potential for the two regimes to diverge over time. Decisions are therefore required as to whether to apply different regimes to different data sets or whether to adopt a common approach. This will be familiar territory for global organisations that currently adopt a 'highest common denominator' standard of privacy compliance across a multitude of jurisdictions but still have to contend with local requirements in some areas, such as breach notification and individuals' rights.

Beyond adequacy - Brexit's wider data privacy implications

Beyond Brexit – Part of the Horizon Scanning series

Regulatory oversight

The end of the transition period will, for some, bring a change in regulatory oversight or additional data protection authorities ('DPAs') to deal with. For example, if a business currently has the UK Information Commissioner ('ICO') as its lead supervisory authority ('LSA'), it should assess whether the EU GDPR's One-Stop Shop mechanism will continue to be available for its EU operations after the end of the transition period. If it will, there will be a new LSA to deal with for the purposes of the EU GDPR, in addition to the ICO for its UK operations. Similarly, an EU business that currently has an EU LSA for its processing activities across the EU (including the UK) will need to deal directly with the ICO, as well as with its current LSA. In some cases, the One-Stop Shop will no longer be available to a business after the transition period – in this case, a number of DPAs may have jurisdiction.

DPAs across the EU already differ in their regulatory approaches and policies, and it is very possible that over time the ICO will diverge even further from the EU DPAs. Having to deal with a new DPA means that businesses will have to take account of new guidance and, more importantly, new approaches to regulation and enforcement. This can impact the risk profile for data privacy compliance, requiring businesses to reassess their 'risky' processing and adjust their own areas of priority to match that of the relevant DPA. For example, the ICO does not appear to have focused significantly on data retention as part of its GDPR enforcement actions to date, but a number of EU DPAs have already issued fines, including for amounts over 2% of turnover, in this area.

Double jeopardy risk for fines

Businesses that become subject to both the EU and the UK GDPR run the risk of being fined under both regimes for the same breach. This will be a change for all those businesses with a UK establishment that currently benefit from the One-Stop Shop. Whilst businesses that continue to have a main establishment in the EU (as well as their UK establishment) risk two enforcement actions, those who cease to benefit from the One-Stop Shop entirely will potentially face multiple enforcement actions from different EU DPAs.

Some businesses could therefore be at risk of receiving maximum fines in multiple jurisdictions. Whilst one might hope that there could be agreement between the ICO and the EU DPAs to avoid this, it is doubtful that there would be the political will to do so. After all, this would effectively require them to agree to play second fiddle to another regulator without the benefit of other co-operation arrangements. The resulting situation is, of course, no different to existing global investigations where a business may be sanctioned, for instance, in the US and the EU for the same incident.

Having said that, the ICO's Regulatory Action Policy says it will take into account ability to pay and financial hardship. It is possible that a large fine from an EU DPA

Beyond adequacy - Brexit's wider data privacy implications

would therefore be factored into the ICO's financial calculations for a fine under the UK GDPR. This would however require the EU fine to be published first and we can't imagine that the ICO would want to delay its own enforcement action, at least in every case.

Representatives

Businesses outside the EEA that are caught by the extra-territorial scope of the EU GDPR are generally required to appoint a representative. After the transition period, this will apply to UK businesses offering goods or services to individuals in the EU or monitoring their behaviour in the EU. Similarly, EU businesses caught by the extra-territorial provisions of the UK GDPR will need to appoint a UK representative.

Those businesses that are already required to have a representative need to assess if they must appoint a second. For example, a non-EEA business that offers goods to individuals in France and the UK will in future need a representative in each jurisdiction in order to satisfy both regimes.

Processing grounds

Where businesses rely on compliance with Union or non-UK Member State law as their legal basis for processing personal data under the EU GDPR, they will need to reassess what lawful bases will be available to them for that processing after the transition period. In some cases, this may mean relying on the legitimate interests ground and completing a legitimate interests' assessment. This may have further unexpected consequences too – for example, relying on this ground is a trigger for the appointment of a data protection officer in one Member State.

A similar issue arises when processing special category data in accordance with a legal basis set out in local law. In the UK for example, Schedule 1 of the Data Protection Act 2018 will no longer be relevant to processing related to the offer of goods or services into the EU. The grounds in local law vary significantly and so, there may be no direct match in the relevant jurisdiction(s), requiring a reassessment of the processing ground and, potentially, reconsidering the processing activity.

Processor terms

Businesses should review contracts with processor terms and consider whether they should be amended, for example, to reflect which GDPR applies to which processing and/or whether references to the GDPR will automatically be replaced by references to the UK GDPR. In some cases, this may mean discussing with counterparty processors or controllers what changes are required.

Adequacy for international transfers

Although, as mentioned above, international transfers have already received significant focus in Brexit planning, this article would not be complete without reference to them given the importance of the free flow of data to businesses.

After the transition period, transfers of personal data from the UK to the EEA will continue to be permitted under UK Brexit-related legislation. Much of the focus has

Beyond adequacy - Brexit's wider data privacy implications

Beyond Brexit – Part of the Horizon Scanning series

therefore been on EEA to UK transfers and whether the UK will obtain an adequacy decision from the EU.

An adequacy decision requires 'essential equivalence' between the EU's and the UK's levels of data protection. Although the enactment of the UK GDPR will support the UK's application for an adequacy decision, there are a number of other factors at play which mean that it is by no means certain that such a decision will be granted before the end of the transition period (or potentially at all). These include EU concerns about the UK's surveillance and intelligence gathering laws (as exemplified for the US in the CJEU Schrems II decision) and COVID-19 delaying negotiations between the EU and other countries applying for adequacy ahead of the UK.

Businesses therefore need to assess what is the most appropriate alternative solution for each current transfer of personal data from the EEA to the UK, including - in particular - the EU's standard contractual clauses ('SCCs'). However, given the doubt cast onto the validity of the SCCs in the Schrems II decision, it will be necessary to assess the nature of any data flows from the EEA to the UK, to determine whether that data flow is (for example) at particular risk of interception by UK authorities and consequently whether any additional steps are needed to adequately protect the information being transferred. Given that putting in place SCCs for, potentially, thousands of contracts requires significant resources, businesses need to determine when they will kick off the implementation phase (and how they will resource it) as time is running out.

Practical steps

With the certainty that the transition period will not be extended, businesses need to put in place and start to implement their Brexit plans now to the extent they have not done so already. This should include:

- Assessing which of the EU and UK data privacy regimes applies to which of their processing, and deciding on a compliance strategy;
- Assessing whether the One-Stop Shop will be available for EU operations and, if so, analysing who will be the LSA for the purposes of the EU GDPR;
- Identifying which DPAs have jurisdiction if the One-Stop Shop does not apply;
- Analysing the impact of a change in risk profile as a result of new or additional DPAs having jurisdiction;
- Reassessing any 'riskier' processing to check whether this still falls within the business's risk appetite or if changes are required;
- Updating risk committees and internal risk protocols to reflect the risk of multiple fines and, where relevant, a change in risk profile;
- Deciding on a contingency plan for international transfers, including implementing SCCs which would comply with the Schrems II decision, and determining the appropriate time to implement this;

Beyond adequacy - Brexit's wider data privacy implications

Beyond Brexit – Part of the Horizon Scanning series

- Identifying whether an EU/UK representative is necessary and taking the necessary steps to make such an appointment;
- Reviewing and updating legal bases for processing where based on Union or non-UK Member State law;
- Identifying and reviewing any EU-wide approach to areas where Member States were permitted to 'tailor' the GDPR (e.g. in relation to exemptions);
- Reviewing processor contracts and, where necessary, updating them;
- Updating privacy notices, where required (e.g. to reflect changes to regulators, different processing grounds, new representatives, etc.); and
- Updating other internal records (e.g. records of processing) to reflect changes, such as to processing grounds.

If you would like further information about this topic, please speak to your usual Slaughter and May contact.

Rebecca Cousin
Partner, Co-head of Data Privacy
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Cindy Knott
Data Privacy Professional Support Lawyer
T +44 (0)20 7090 5158
E cindy.knott@slaughterandmay.com