December 16, 2020

‘Inadequacy’ – an inevitable end to 2020?

With Brexit on the horizon, potential changes to data transfer laws raise the spectre of disruption to personal data transfers from the European Economic Area (EEA) to the UK.

Attorneys
Clare Sellars
Rohan Massey

From 1 January 2021, the UK will be considered a third country outside of the EEA for the purposes of the General Data Protection Regulation (EU) 2016/679 (GDPR). Ahead of this deadline, businesses should start thinking pragmatically about personal data transfers from the EEA to the UK to ensure a frictionless transition in case a European Commission 'adequacy decision' is delayed, or worse, not granted at all.

So what is ‘adequacy’?

European Commission ‘adequacy decisions’ constitute findings by the Commission that the legal frameworks and data protection regimes of countries, territories, sectors or international organisations outside the EEA are ‘essentially equivalent’ to those established by the GDPR and provide ‘adequate’ protection for individuals’ personal data.

The UK is currently undergoing an adequacy assessment. If an adequacy decision is granted in respect of the UK prior to 1 January 2021, personal data will be able to continue to pass freely between the UK and the EEA. If not, EU-based organisations will be required to implement additional appropriate safeguards in order to transfer personal data from the EEA to the UK. By failing to act, companies could face enforcement action of various kinds (including, in the case of very serious breaches, maximum penalties of the greater of €20 million or 4% of annual global turnover).

Adequacy decisions take time. The fastest assessment carried out to date, for Argentina, took 18 months. Whilst the Political Declaration—which sets out the framework for the future relationship between the EU and the UK—implies that such a decision may be reached for the UK before 31 December 2020, this appears increasingly unlikely. The reality is that it could be upwards of two years before the UK assessment is complete and a decision regarding adequacy is made.

The 20 million Euro question: how likely is an ‘adequacy decision’ for the UK?

On the face of it, the ‘spirit’ of the GDPR is encompassed in the Data Protection Act 2018 (DPA18) and the UK GDPR. However, there are some important challenges.

A key obstacle is UK law enforcement’s reliance on mass surveillance under the Investigatory Powers Act 2016. This was most recently highlighted when the European Court of Justice (ECJ) ruled in October 2020 (in joint cases C-511/18, La Quadrature du Net and Others, C-512/18, French Data Network and Others, and C-520/18, Ordre des barreaux francophones et germanophone and Others) that mass surveillance by national security agencies is unlawful. The US also encountered this when the Court of Justice of the European Union (CJEU) invalidated the EU-US Privacy Shield adequacy decision on this basis earlier this year. Therefore, even if an adequacy decision is granted, legal challenges by data privacy activists may well be made, with subsequent invalidation a possibility. On the other hand, some comfort can be taken from the fact that Japan has similar (if not more pervasive) surveillance laws in place, and was awarded adequacy in January 2019.

The ‘immigration control’ exemption in the DPA18 may also cause concern. This exemption allows the UK government to use personal data without a data subject’s consent, for the purpose of ‘effective immigration control’. However, in 2019, citizens’ rights groups lost a challenge against the exemption in the High Court of England and Wales on the basis that the DPA18 was appropriate and the safeguards were sufficient to remedy any errors. Nonetheless, this was a

decision made under the jurisdiction of England and Wales, and not European law. The EU may well take a different approach.

If no adequacy then what?

Assuming that no adequacy decision is granted in respect of the UK before the end of the transition period, 'business as usual' transfers of personal data between the EEA and the UK require swift attention. It is the responsibility of businesses making or planning to make such transfers to consider implementing appropriate safeguards. Some examples are set out below:

Standard Contractual Clauses (SCCs). SCCs are currently the most commonly used and cost-effective safeguard to ensure adequate protection for personal data transferred outside the EEA. The SCCs are standard sets of contractual terms which are entered into by importers and exporters of personal data. They are approved by the European Commission and ensure that any transfers comply with the GDPR's requirements regarding international personal data transfers.

However, SCCs are currently the subject of review and debate and the European Commission has recently published new draft sets of SCCs which are open for public consultation. The proposed new SCCs adopt a flexible, modular approach and significantly improve on the current SCCs. The new SCCs should make international personal data transfers much easier (at least once the initial administrative hurdle is cleared).

In addition, in the *Schrems* II case in July 2020 (C-311/18), the CJEU ruled that SCCs (and other transfer tools) could continue to be used to transfer personal data outside the EEA if 'additional safeguards … that supplement the [SCCs]' in order 'to compensate for the lack of data protection in a third country' are implemented, if required. Such supplementary measures will be required if, following an assessment of the laws and practices of the third country of destination of the transferred data, anything is revealed that might impinge upon the effectiveness of the appropriate safeguards of the transfer tools relied upon. The European Data Protection Board (EDPB) has recently released draft guidance (again, currently subject to public consultation) which explains what appropriate supplementary measures might include. The guidance notes that technical, contractual and/or organisational measures can be adopted to meet the standards required, and often a combination of such measures will be appropriate.

However, the guidance also notes that contractual and organisational measures alone are unlikely to be sufficient to demonstrate essential equivalence, and, in some cases, only technical measures (e.g. encryption) will be appropriate. The guidance also notes that there are also certain circumstances (such as transfers of non-encrypted personal data to cloud providers in certain third countries) where even technical supplementary measures are unlikely to be sufficient to provide adequate protection for personal data transferred from the EU.

Binding Corporate Rules (BCRs). For multinational companies, BCRs are a tailor-made alternative to the impracticalities of implementing numerous SCCs between different group companies. Through legitimising ex-EEA as well as intra-group transfers, they offer an effective way for data-reliant organisations to perform hundreds of personal data transfers on a daily basis.

Explicit consent and other derogations. In the absence of an adequacy decision or appropriate contractual and legal safeguards, a transfer of personal data from the EEA to the UK may still be possible if one of the derogations set out in Article 49 of the GDPR can be relied upon. The most commonly relied upon derogations include the obtaining of explicit consent from data subjects, the fact that the transfer is necessary for the performance of a contract between the data subject and the controller, and circumstances where the transfer is necessary for reasons of important public interest. However, whilst more straightforward, firms should consider the EDPB's position on the GDPR's derogations, which highlights the fact that the derogations may only be relied upon in limited circumstances.

Confused? Don't worry—you are not alone! We are monitoring developments and market practice to enable us to provide advice on how best to achieve personal data transfers to the UK in various circumstances.

What does this uncertainty mean for businesses?

On the basis that an 'adequacy decision' by the European Commission may not be forthcoming, businesses should act now to consider how best to ensure that personal data can continue to flow from the EEA to the UK from 1 January 2021. At best, the UK will receive an adequacy decision. At worst, inaction threatens significant disruption to the free flow of personal data from Europe to the UK. If Brexit reaches an inadequate conclusion, don't let your business suffer the same fate.

Please contact Clare Sellars, Rohan Massey, Abbey Shaw or the Ropes & Gray attorney who usually advises you with any questions you may have or if you would like additional information.