Data Privacy and Cybersecurity

Is the UK's Data Privacy Adequacy Decision in Doubt?

By: Kelly Hagedorn and Tracey Lattimer

Introduction

On 31 January 2020, the United Kingdom (UK) left the European Union (EU). Until the end of 2020 (known as the "transition period", during which the UK and the EU attempt to negotiate a post-Brexit deal), however, EU laws and rules will continue to apply in the UK and any reference to the EU in legislation is deemed to include the UK. Accordingly, until 31 December 2020, the General Data Protection Regulation (Regulation (EU) 2016/679) (the GDPR) will continue to apply in the UK. From 1 January 2021 onward, however, the UK will be deemed a third-country for the purposes of the GDPR, which may have a significant impact on the flow of data between the European Economic Area (EEA) and the UK.

Cross-border data transfers under the GDPR

Under the GDPR, transfers of personal data outside of the EEA to a third-country may only take place if: (a) the European Commission has issued a decision declaring that the third-country ensures an adequate level of protection to personal data (an Adequacy Decision)[1]; (b) "appropriate safeguards" are put in place to protect personal data (including, for example, binding corporate rules or standard contractual clauses); or (c) one of the specific derogations set out in the GDPR apply.

Obtaining an Adequacy Decision for the UK as part of a negotiated post-Brexit deal would be the most convenient outcome for UK businesses, as transfers of personal data could continue to take place freely between the EEA and the UK without further safeguards or measures being required. The provision of an Adequacy Decision forms part of the negotiations between the UK and the EU, but there is doubt as to whether a decision will be issued by 1 January 2021, if ever.

Obstacles to the UK obtaining an Adequacy Decision

In February 2020, the European Parliament issued a document (known as a resolution) which addressed the EU's proposed mandate for negotiating a new partnership with the UK and which raised a number of concerns regarding the UK's current data protection regime. In particular, the resolution raised concerns with:

1. the fact that the UK's Data Protection Act 2018 (DPA 2018) contains a general and broad exemption from the data protection principles and data subjects' rights for the processing of personal data for immigration purposes, which exemption conflicts with the GDPR;
2. the UK's legal framework on the retention of electronic telecommunications data, which "*does not currently meet the conditions for adequacy*"; and
3. the UK's legal framework in the fields of national security and the processing of personal data by law enforcement authorities, noting that mass surveillance programmes "*might not be adequate under EU law*".

The resolution instructed the European Commission, when considering whether to grant an Adequacy Decision to the UK, to "*carefully assess UK's data protection legal framework and ensure that the UK has resolved the problems identified in this resolution prior to considering UK data protection law adequate*".

Johannes Caspar, head of the Hamburg Data Protection Authority, who is said to be advising the European Commission on any Adequacy Decision with the UK, has reportedly made similar comments: "*When assessing the adequacy level, the crucial point will be the UK's surveillance activities and their participation in the "Five Eyes" network…If the UK continues its large-scaled surveillance practice, it is doubtful whether the Commission can adopt an adequacy decision.*"

Whilst the UK's surveillance practices are not new, up until now, the UK has benefited from the freedom afforded to EU member states to implement their own independent national security policies. Now that the UK is no longer a member of the EU, such national security practices and policies are more open to scrutiny.

An additional potential barrier to the UK obtaining an Adequacy Decision is the written statement published by Boris Johnson in February 2020 on the UK Government's proposed approach to negotiations with the EU. In his statement, Mr Johnson said that the UK "*will in future develop separate and independent policies*" in a number of areas, including data protection. If, for example, the UK's data protection laws were to diverge significantly from the GDPR, this could jeopardise an Adequacy Decision.

Despite these potential obstacles, in March 2020, the UK Government published an "Explanatory Framework for Adequacy Discussions", in which it emphasised that the UK has a "*world-class*" data protection regime. Key to the UK Government's belief that the UK's data protection regime meets the standard of "essential equivalence" required for an Adequacy Decision is that, following the transition period, the UK's main data protection legislation will consist of the DPA 2018 and the "UK GDPR", which will essentially write the GDPR into UK law with necessary changes to tailor its provisions to the UK. However, the Explanatory Framework also noted that the Government considers the UK to have "*robust rules for law enforcement and national security processing*" and that "[t]*he UK's data protection legislation provides unprecedented independent oversight of the activities and conduct of the UK's law enforcement framework, national security framework, and investigatory powers.*" Such comments do not suggest that the UK Government intends to amend any of the UK's national security policies or legislation, despite the concerns raised by the European Parliament. It remains to be seen whether the totality of the comments made in the Explanatory Framework will allay the concerns of the European Parliament and the European Commission.

Options if the UK does not obtain an Adequacy Decision

If the UK is unable to obtain a full Adequacy Decision by the end of 2020, or at all, one option may be the agreement of a partial Adequacy Decision, similar to the decisions in place for Canada and the United States. Canada's Adequacy Decision, for example, applies only to private entities that fall within the scope of the Canadian Personal Information Protection and Electronic Documents Act. The United States' Adequacy Decision applies only to companies that participate in the EU-US Privacy Shield. Such a partial Adequacy Decision could, for example, bypass the European Parliament and European Commission's concerns regarding the large-scale transfer of personal data between foreign law enforcement agencies, whilst allowing the continued free flow of personal data between private entities.

Without any form of Adequacy Decision, UK entities will need to rely on "appropriate safeguards" to continue to freely receive personal data from the EEA. For example, binding corporate rules could be implemented to allow for the transfer of personal data between entities within the same group structure. Alternatively, UK entities will need to enter into standard contractual clauses with each entity in the EEA from which they receive personal data.

Companies should be planning now for what may happen if the UK does not receive an Adequacy Decision.

---

[1] To date, the European Commission has issued 13 Adequacy Decisions in respect of the following

countries: Andorra, Argentina, Canada (commercial organisations only), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, Uruguay and the United States (EU-US Privacy Shield certified organisations only).

Contact Us

Kelly Hagedorn

khagedorn@jenner.com | Download V-Card

Tracey Lattimer

tlattimer@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

David Bitkower
Chair
dbitkower@jenner.com
Download V-Card

David P. Saunders
Co-chair
dsaunders@jenner.com
Download V-Card