

WHAT FUTURE FOR UK-EU DATA FLOWS?

Date: 28 October 2020

EU Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Noirin M. McFadden, Keisha Phippen

With the Brexit transition period ending on 31 December 2020, and no deal in sight, the future of cross-border data transfers between the European Economic Area (the EEA) and the United Kingdom remains unclear. On 1 January 2021, the United Kingdom will be considered as a “third country” and, unless a Brexit deal is proposed dealing with data protection and how data transfers between the EEA and the United Kingdom are to be treated, it could be significantly more difficult for European Union (EU)-based entities to transfer personal data to the United Kingdom.

Under [Article 44](#) of the [General Data Protection Regulation](#) (GDPR), there is a general prohibition on the transfer of personal data from within the EEA to recipients in a jurisdiction outside the EEA. Among the exceptions to this general prohibition, an “adequacy decision” granted by the European Commission would prove to be the least cumbersome solution for business continuity, as once a third country has been granted such a status, it can pass personal data freely between it and the EEA without any additional safeguards being required. However, such adequacy decision may only be granted upon review by the European Commission and confirmation that the third country in question protects personal data to the same standard as provided for in European law. As of today, Japan is the only country to have received such adequacy decision under GDPR¹ (see our alert [here](#)).

Separate from ongoing trade negotiations, determining whether personal data transfers from the EEA to the United Kingdom may continue freely has been the subject of much debate over the course of this year and, at the moment, it appears increasingly unlikely that an adequacy decision will be in place by the end of the year. If so, then as of 1 January 2021, there will be no mechanism in place to automatically allow the EEA to pass personal data to the United Kingdom. Businesses and organizations will have to take specific steps to provide safeguards for personal data they need to transfer to the United Kingdom.

UK government ministers and officials appear to remain hopeful that an adequacy decision will be granted, but their public statements also sound a note of caution. Paul Gaskell, a deputy director at the EU Exit Data Protection Negotiation Hub within the Department of Digital, Culture, Media and Sport, [told a conference recently](#) that he still expects the European Commission to grant an adequacy decision. Despite this assurance, Gaskell also warned EU companies, or companies headquartered in the United Kingdom with operations in the EU, to “act now” to ensure they have all the necessary legal mechanisms in place should no data adequacy deal be reached. Department of Digital, Culture, Media and Sport minister John Whittingdale gave a similarly optimistic assessment of the United Kingdom's chances of an adequacy decision in [a response to a parliamentary question](#), stating that “it is self-evidently in the interest of both sides to have adequacy decisions in place by the end of the year” and that “no other third country's standards have ever been closer to the EU's”. However, this was undercut by his admission that “we will take sensible steps to prepare for a situation where decisions are not in place by the end of the transition period.”

The European Commission continues to consider whether to grant an adequacy decision to the United Kingdom, and businesses anxiously await the outcome of this process. The United Kingdom has incorporated the GDPR into its own law post-Brexit, which will be in its favor in securing adequacy status. However, the European Commission will also be weighing up factors that weaken perceptions of the United Kingdom's commitment to data protection, including the United Kingdom's invasive intelligence-gathering laws (more on that below) and the possibility that the UK government intends to water down its version of the GDPR in future, as hinted at the recently published [national digital strategy](#). Ultimately, it will be for the United Kingdom to decide how closely it wishes to cleave to EU data protection norms for the sake of an adequacy decision. Yet at a time when those norms are being adopted across the globe, including [potentially in the United States](#), moving away could mean that UK businesses could face many additional barriers to maintaining international flows of data.

In the event that the United Kingdom is not granted this adequacy decision, businesses and organizations will have to rely upon other exceptions outlined in the GDPR. Aside from consent of the data subjects, which should rarely be a preferred option due to its intrinsically precarious nature, or other circumstantial exceptions, two should be considered:

The first of these would consist of Standard Contractual Clauses, which are individual agreements containing contractual obligations on the data exporter and the data importer, and rights for the individuals whose personal data is transferred. Standard Contractual Clauses safeguard EU data protection standards between the two parties taking part in a transfer. This solution, despite the limitations discussed below, remains the fastest solution to implement for organizations.

The second option would be for businesses and organizations to make use of the Binding Corporate Rules framework. Binding Corporate Rules are internal rules that facilitate cross-border data transfers within a multinational group of companies and international organizations. This solution generally requires substantial investment in time and resources for its implementation and only addresses data transfers within an organization, excluding relationships with service providers, for example.

However, the recent decision from the Court of Justice of the European Union (CJEU) in the *Facebook Ireland Ltd. v. Maximilian Schrems* case, dated 16 July 2020 ([Schrems II](#); see our alert [here](#)), which held that Standard Contractual Clauses, while remaining valid, would only be a suitable mechanism for the transfer of personal data outside of the EEA if:

- In practice they guarantee the same level of protection as the personal data would enjoy in the EU; and
- The clauses are sufficient to protect personal data transfers in instances where the law of the third country allows its intelligence and security services to access such data.

The CJEU made it clear in its decision that if the law in the destination country means that the recipient of the personal data cannot guarantee it will be able to comply with Standard Contractual Clauses terms, or if there are other reasons why the Standard Contractual Clauses will not adequately protect the data, then the transfer must be stopped. Although the decision did not explicitly refer to Binding Corporate Rules, it is likely that the same reasoning would apply to them.

The Standard Contractual Clauses are currently under review to address necessary updates that account for the GDPR and the fallout from Schrems II. Although Schrems II considered the effect of the United States' security laws on data transfers, the United Kingdom's laws permit similarly invasive intelligence gathering powers, which

could lead to issues for data transfers from the EEA post-Brexit. As such, organizations may also need to put in place additional safeguards alongside Standard Contractual Clauses and Binding Corporate Rules to ensure an adequate level of protection for personal data transferred from the EU to the United Kingdom.

In anticipation of a “No-Deal Brexit,” organizations will need to ensure that personal data is legitimately transferred to the United Kingdom following the cessation of the transition period on 31 December 2020.

The K&L Gates data protection team remains available to assist you in achieving compliance of your data transfers at a global level. Please get in touch if you would like to discuss the steps that your organization might want to consider to prepare now for the end of the transition period.

FOOTNOTES

¹ Ongoing adequacy decisions under the pre-GDPR framework include Andorra, Argentina, Canada (commercial organizations only), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland, and Uruguay. Adequacy talks have been ongoing with South Korea for 18 months.

KEY CONTACTS



CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM



NOIRIN M. MCFADDEN
STAFF LAWYER

LONDON
+44.20.7360.8135
NOIRIN.MCFADDEN@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.