



Data Privacy Detective Podcast – Episode 67: Data Flows After Brexit... For Now

Jul 01, 2021

Categories:

[Blogs](#)

[Podcast](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

On June 28, 2021, the Europe Union granted two adequacy decisions to the United Kingdom for personal privacy purposes.

- [Decision on the adequate protection of personal data by the United Kingdom: General Data Protection Regulation | European Commission \(europa.eu\);](#)
- [Decision on the adequate protection of personal data by the United Kingdom: Law Enforcement Directive | European Commission \(europa.eu\).](#)

This assures, for now, that data flows between the EU and UK can continue without restrictions. But for the first time, the EU's decisions were *not permanent* and will last only four years. What's going on?

Because of Brexit, the UK and the EU reached a transition agreement at the end of 2020. This included six months for the UK and EU to reach an agreement about data privacy flows. The deadline approached, and the EU decision was made just in time (the UK had already issued its own adequacy decision regarding data going to the EU). Had it not been made, one estimate was that UK businesses would face immediate compliance costs of about 1.6 billion pounds, aside from other costs. So, UK businesses can rest easy – for a time. According to [Kim Walker, a leading UK privacy attorney](#) at the firm of Shakespeare Martineau, 11% of global data flows through the UK, and 70% of UK data flows through the EU.

Why the last-minute timing and why the unusual temporary grant of an adequacy decision? The answer lies in the same surveillance issues that restrict data flows between the EU and the United States. Without a comprehensive and protective federal personal data privacy law, the United States is unlikely to receive an adequacy decision from the EU indefinitely. The EU is particularly skeptical of mass surveillance by U.S. authorities. The British mass

surveillance system is not that different from the American approach to how and when public authorities can access private personal information. The EU is concerned that by granting adequacy to the UK, this could create a back door for the UK to grant unrestricted data flow to the United States, thus undermining Europe's basic GDPR approach to restricting data flows that may disrupt the protections of personal privacy at the heart of GDPR.

The UK is keen to escape control by the EU Court of Human Rights. That court has over-ridden U.S./EU Commission safe harbor and other measures through two "Schrems" decisions that agreed with an Austrian privacy crusader about data flows between EU and U.S. business. The EU is suspicious that the UK will seek an agreement with the U.S. on a bilateral trade agreement and, in that connection, will sacrifice GDPR standards in the bargaining. Hence, the 4-year limitation in the adequacy grant.

What practical impacts? Kim Walker provided some suggestions at a July 1 event of PrivacyRules, a global alliance of tech and law firms. www.privacyrules.com. U.S. businesses should not assume that a back door is now opened to get EU data from the UK that it could not get directly from EU sources. UK business should be extremely cautious in providing to sources outside of the EU data that is not consistent with GDPR regulation (along with Switzerland and other countries considered adequate by the EU). It is probably that Mr. Schrems or another privacy advocate or organization will challenge in the EU Court of Human Rights the UK adequacy decision, at a minimum to establish that no UK business that obtains EU data can simply send it off to other countries without concern. For businesses in countries not considered adequate by the EU, their choices can include entering a negotiated system (like the Privacy Shield Framework of the U.S., EU and Switzerland) or using Standard Contractual Clauses prescribed by the EU for business compliance with GDPR standards.

This unfolding clash of national and supranational systems shows that the world is far behind the flow of data. The internet faces splintering, the rise of national data walls, increased compliance costs for businesses dealing with global data flows, the uncertainty from us all about the very meaning of our privacy in a world of

digital data.

If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.