NO RISK TOO SMALL: AUSTRIAN DATA PROTECTION AUTHORITY STANDS FIRM BEHIND DATA TRANSFER ROADBLOCK

Matt L. Rotert

On April 22, 2022, the Austrian data protection authority (the "Datenschutzbhorde" or "DSB") upheld its January 2022 decision, finding that transfers of personal data from the EU to U.S.-based Google could not be supported by Standard Contractual Clauses ("SCCs") – even with supplementary measures in place.

Transferred Personal Data Could be Subject to U.S. Intelligence Requests

The April 22, 2022, DSB decision does not create an absolute bar on transfers of personal data to the U.S. It does, however, represent a significant roadblock when such transfers are based solely on SCCs. The DSB's prior determination that transfers of personal information from the EU to Google based on SCCs were not valid was based on the potential for a FISA 702 request from U.S. intelligence agencies. Because any entity that is identified as an "electronic communication service provider" can be subject to a FISA 702 request, the DSB decision will have far reaching consequences for two reasons.

First, the definition of an "electronic communication service provider" is likely very broad. For example, the U.S. Department of Justice ("DOJ") has defined electronic communications service provider to mean "any company or government entity that provides others with the means to communicate electronically can be a 'provider of electronic communications services'… regardless of the entity's primary business of function." In doing so the DOJ referenced legal opinions finding employers that provided email service to employees and a city that provide pager services to police offices to be "electronic communication service providers." Under this definition, essentially any entity receiving digital personal information from the EU will likely be considered an "electronic communication service provider."

It is unlikely that any EU data protection authority will take a more narrow view.

Second, the definition of data subject to FISA 702 is also likely very broad. Here, the DSB stated that "the scope of application of FISA 702 is to be understood *very* broadly and the powers of US authorities extend to *all* data in the company due to a minor activity within the scope of application of FISA 702."

Once an entity is determined to be an electronic communications service provider, therefore, U.S. intelligence agencies would be assumed to have access to any data within the control of that entity – even if that data is not otherwise connected to the electronic communication.

In short, if a U.S. entity can be identified as an "electronic communication service provider," that entity cannot receive personal data from the EU based solely on SCCs because such information would be available to U.S. intelligence operations.

The Likelihood of a U.S. Intelligence Request is Immaterial

The April 22, 2022, DSB decision also provided additional analysis that may erode the most plausible defense for continuing to transfer personal data from the EU to the U.S – namely, that the data subject to transfer is unlikely to be subject to a request from a U.S. intelligence agency. Here the DSB determined that Article 44 of the GDPR did not allow data protection authorities to consider the likelihood of harm when determining whether the local laws of a third country provide adequate protection. The decision is binary: either adequate protection could be provided, or it could not.

Because the United States does not have a current adequacy decision and the DSB had previously determined that SCCs that are not binding on the U.S. government cannot provide adequate protection, the DSB decision confirmed: (1) that it is unlikely that transfers of personal data to the United States can be supported by SCCs; and, (2) that transferring entities cannot disregard the DSB's decision simply because the data is unlikely to be of interest to U.S. intelligence agencies.

Future Impact

The immediate impact of this decision is that transfers of personal data from Austria to the United States will be unlikely to survive scrutiny by the DSB. The DSB decision, however, should be viewed as a sign of what is to come and not as an outlier. To be clear, absent an adequacy decision to replace the Privacy Shield invalidated by *Schrems II*, there are likely to be limited valid methods for the routine transfer of personal data from the EU to the U.S.

The rationale for the April 22, 2022, DSB decision may also cast a shadow on any adequacy decision based on the recently announced agreement in principle on a new Trans-Atlantic Data Privacy Framework (a/k/a "Privacy Shield 2.0").

Based on the April 22, 2022, DSB decision, as long as a data protection authority or the Court of Justice for the European Union (the "CJEU") can identify at least some risk that personal data transferred to the U.S. could be accessed by U.S. intelligence agencies, the adequacy decision will likely be invalidated.

Additionally, the April 22, 2022, DSB decision made clear that arguments regarding the economic and political impact of finding a transfer unsupported (or unsupportable) are untenable. Even if the European Commission considers the economic impact of not giving the U.S. an adequacy decision based on the Trans-Atlantic Data Privacy Framework, therefore, nothing requires data protection authorities (or the CJEU) to abide by that consideration.

The net takeaway is that if the Trans-Atlantic Data Privacy Framework merely reduces the risk of access to personal data transferred from the EU to the U.S. without removing that possibility, the new framework will likely be seen to suffer from the same flaw as the Privacy Shield framework before it and be deemed invalid, and SCCs will continue to be found insufficient.

For additional information on this topic, please contact **Matt Rotert** at mrotert@redgravellp.com. For further details on Redgrave LLP's Data Privacy services, please contact **Martin Tully** at mtully@redgravellp.com or at 773.782.0352 .

Redgrave LLP *is one of the largest legal practices focused exclusively on addressing the legal challenges that arise at the intersection of the law and technology, including eDiscovery, information governance, and data privacy. We employ some of the most experienced professionals in the field. We provide clients with practical, innovative, and cost-effective solutions and serve Global and Fortune 500 companies across a diverse array of industries. We also work collaboratively with Am Law 100 law firms in roles ranging from co-counsel to consulting and testifying expert witnesses and have appeared in state and federal courts throughout the United States.*