SQUIRE PATTON BOGGS

EU Data Transfers Post-Schrems II:

What are the Viable Options Going Forward?

Key Takeaways

Thank you for your interest in our virtual Roundtable Discussion on the implications of the Schrems II decision that took place on July 30, 2020. Given the high level of participation, clearly this topic is on the minds of companies across all sectors.

Below we share with you key takeaways from the Roundtable.

1. The **Privacy Shield has been declared invalid** by the European Court of Justice (CJEU). We expect that Supervisory Authorities (SAs) in Europe will move to enforce the judgment in a proportionate way, giving a reasonable amount of time for Privacy Shielded companies to put in place acceptable alternative arrangements. SAs have a wide range of enforcement levers available to them under the GDPR, including issuing warnings, imposing administrative fines and suspending or banning data transfers. The US government, for its part, continues to consider the Privacy Shield to remain in effect. Privacy Shielded companies should take care to follow the Privacy Shield withdrawal procedures in line with their commitments, unless alternative instructions are issued by the U.S. Department of Commerce.

2. The CJEU concluded that the **Standard Contractual Clauses remain valid in principle, but each transfer arrangement must be assessed on a case-by-case basis** to determine whether the data importer can, in fact, uphold its contractual obligations in line with the local laws to which it is subject. **This requirement applies to transfers not only to the US, but also to all countries where there is not a valid "adequacy" decision issued by the European Commission in place**. In regard to US transfers, the bar will be set rather high in light of the CJEU's conclusions on Privacy Shield. The main focus of the CJEU's concern is the ability of US government agencies to engage in the bulk collection of personal data of EU residents without any effective right of recourse, in light of the broad powers of US national security agencies to collect data about foreign nationals under the FISA Amendments Act 2008. Key objectives of investigations carried out under the Act are to facilitate investigations related to counterterrorism, proliferation of weapons of mass destruction, protection of US troops and protection against cybersecurity attacks by foreign actors. Telecommunications carriers and software-as-a-service ("remote computing") companies have particular obligations under the Act.

3. It remains to be seen whether the SCCs can be used to legitimize *any* transfers of personal data to the US, and the type of supplementary measures Supervisory Authorities will require if the laws of the country of destination do not enable the data importer to comply with the SCCs or BCRs using a risk-based approach. In light of the CJEU's judgment, all eyes will be on the Irish Courts and the Irish Data Protection Commissioner, which must now decide how to apply the judgment to the facts of the case before them. In the meantime, **companies relying on (or planning to switch from Privacy Shield to) the SCCs should identify and risk-assess all personal data transfers made under the SCCs, with a priority on EU/UK to US transfers**. In line with the GDPR's Accountability Principle, EU-based data exporters will be responsible for carrying out this assessment in cooperation with the relevant data importers.

4. The European Data Protection Board has indicated that the **Binding Corporate Rules should be considered in the same light as the SCCs**.

5. The GDPR also provides various **derogations (exceptions) that may be appropriate to use in specific circumstances**, where SCCs, BCRs or bespoke SA-approved data transfer agreements are not available. However, legal defense and contract derogations cannot be used for routine and repetitive transfers. Furthermore, the consent derogation would need to fulfill all of the GDPR requirements for valid consent, in addition to those required by the derogation itself.

The *Schrems II* decision is still being digested by governments and regulators on both sides of the Atlantic. We will continue to provide updates and guidance as developments unfold. If you have specific questions relating to your organization, please feel free to reach out to your usual firm data protection advisor or one of our panelists.

For continued updates on this, as well as other news and insights on cybersecurity, privacy and data protection regulations and developments impacting businesses around the globe, subscribe to our blog, Security & Privacy//Bytes.

Rosa Barcelo
Co-Chair, Data Privacy & Cybersecurity Practice
Partner, Brussels
T +322 627 1107
E rosa.barcelo@squirepb.com

Ann J. LaFrance
Co-Chair, Data Privacy & Cybersecurity Practice
Partner, New York
T +1 212 872 9830
E ann.lafrance@squirepb.com

Francesca Fellowes
Director, Leeds
T +44 113 284 7459
E francesca.fellowes@squirepb.com

Lauren Kitces
Associate, Washington, DC
T +1 202 457 6427
E lauren.kitces@squirepb.com

Mareike Lucht
Associate, Berlin
T +33 1 5383 1167
E mareike.lucht@squirepb.com

Catherine Muyl
Partner, Paris
T +33 1 5383 1167
E catherine.muyl@squirepb.com