Lowenstein Sandler

Privacy & Cybersecurity

January 22, 2021

Post-Brexit, *Schrems II*, and the GDPR: Privacy Compliance Priorities in Early 2021

By Mary J. Hildebrand CIPP/US/E, Edgar R. Hidalgo CIPP/US, and Carly S. Penner CIPP/US

On December 31, 2020, the Brexit transition period ended and the United Kingdom's (UK) domestic implementation of the GDPR, the UK Data Protection Act 2018, as amended (UK GDPR), now governs the processing of personal data in the UK.

As if the UK's separation from the European Union (EU) was not enough to muddle the privacy compliance landscape for U.S. companies doing business in the EU and the UK, the mid-year *Schrems II* decision by the Court of Justice of the European Union (CJEU) that invalidated the EU-U.S. Privacy Shield also ushered in a round of regulatory guidance from both the European Data Protection Board (EDPB) and the European Commission (EC).

On November 10, 2020, the EDPB released recommendations on what the *Schrems II* court referred to as "supplemental measures" to be taken by entities relying on Standard Contractual Clauses (SCCs) as a valid data transfer mechanism. Just one day after the EDPB released its guidance, the EC published drafts of new versions of the SCCs aimed at replacing the existing form SCCs for data transfer outside the EU, as well as wholly new form SCCs to be entered into between all controllers and processors under GDPR Article 28. And most recently, on January 15, 2021, the EDPB and the European Data Protection Supervisor (EDPS) adopted joint opinions on the proposed draft SCCs, concluding that the drafts presented a reinforced level of protection that was intended to address some of the main data privacy and security issues identified in the *Schrems II* decision.

These significant developments at the close of 2020 and turn of the year charted a course in privacy compliance for companies doing business in Europe to take in early 2021. In this two-part Client Alert, the Lowenstein privacy team will explore this compliance "to do" list in more detail–starting with this first installment, ***Part I: Brexit, the GDPR, and a UK Adequacy Decision***.

Part I: Brexit, the GDPR, and a UK Adequacy Decision

Data protection in the UK is now regulated by the UK GDPR and the GDPR no longer applies. The good news is that the UK GDPR is essentially identical to the GDPR, although differences are inevitable over time as the UK Information Commissioner's Office (ICO) and courts interpret and enforce the regulation. However, companies that implemented GDPR compliance programs will need to update their privacy policies, privacy disclosures and other GDPR-related processes to ensure compliance under the UK GDPR. If nothing else, companies will need to update references to the EU and the GDPR to explicitly address the UK and the UK GDPR. Another particularly important requirement under the UK GDPR for companies without a physical presence in the UK is the engagement of a UK representative that is separate from the EU representative named under the GDPR.

The most anticipated post-Brexit consideration in the privacy sphere has been whether the EU will determine that the UK provides an adequate level of data protection. This adequacy designation, held by very few countries worldwide including Israel, Canada and South Korea, would eliminate any need for companies transferring personal data between the UK and EU member countries to rely on the SCCs or any other approved data transfer mechanism for the valid transfer of data.

Although that adequacy decision is still pending, the trade negotiations between the UK and the EU that began shortly after Brexit formally ended

on December 24, 2020 with the *EU-UK Trade and Cooperation Agreement (TCA)* being approved in principle. While the TCA has not yet been ratified by the parties and in any case does not provide an adequacy decision on the UK, it does implement transition measures that allow data flows to continue unimpeded between the EU and the UK for the time being. This is a welcome, albeit temporary, reprieve for companies with data flows between the UK and the EU, but certainly a matter to keep a close eye on.

Next week we will circulate ***Part II: Draft SCCs and Post-Schrems II Regulatory Guidance***, which will focus on the draft SCCs and the impact on U.S. companies of the EDPB and EDPS opinions.

About Us

In today's digital world, where data has become a key asset for conducting business, companies continue to face greater privacy and cybersecurity challenges. At Lowenstein Sandler, our Privacy & Cybersecurity team helps clients navigate the rapidly evolving, increasingly complex privacy and security law landscape in the United States, the EU, and around the world. We deliver innovative privacy and security solutions that meet our clients' critical business needs including the commercialization of data assets in a legally compliant manner. Our targeted counsel is relevant to companies across diverse industry sectors, and public and private companies from start-ups to global enterprises.

Contacts

Please contact the listed attorneys for further information on the matters discussed herein.

MARY J. HILDEBRAND CIPP/US/E
Partner
Chair, Privacy & Cybersecurity
T: 973.597.6308
mhildebrand@lowenstein.com

EDGAR R. HIDALGO CIPP/US
Counsel
T: 973.422.6418
ehidalgo@lowenstein.com

CARLY S. PENNER CIPP/US
Associate
T: 973.597.2516
cpenner@lowenstein.com