Technology, media and telecommunications services after 'Schrems II'

Jul 27, 2020 Save This ()

Lothar Determann Lothar Determann

Editor's Note:

This is the seventh in a series of guidance notes on what the “Schrems II” decision means for companies that rely on EU-U.S. Privacy Shield, controller-to-processor standard contractual clauses, SCCs for transfers to controllers, derogations/exceptions to transfer restrictions, and binding corporate rules, as well as what “Schrems II” means for Brexit and what companies can expect with the road ahead on these issues.

Most companies consider cross-border data transfer restrictions under EU data protection laws a difficult compliance requirement, particularly since July 16, when the Court of Justice of the European Union ruled on the EU-U.S. Privacy Shield and standard contractual clauses. Additionally, companies that offer data-processing services are also facing a difficult sales topic, which commands urgent attention, particularly in the technology, media and telecommunications sectors.

'Schrems II' as a sales versus compliance topic

other services they are using for employee and customer data. Not only providers of information technology services are affected, but more and more products also come with connectivity, remote access for tech support and other data-processing features.

Also, within affiliated groups, companies provide services to subsidiaries and parent companies. To succeed in selling data-processing services and features, companies have to help their customers overcome compliance concerns. Thus, companies not only have to address their own compliance obligations, but they also have to help customers and subsidiaries address their concerns.

Supplementary measures and verification duties

In "Schrems II," the CJEU notes the limitations that SCCs inevitably have. Contracts can bind only the contracting parties, but not government authorities or others that might threaten data privacy. Therefore, the CJEU states in Sections 133 and 134 of the judgment, companies in the EU may need to adopt "supplementary measures" and "verify, on a case-by-case basis and, where appropriate, in collaboration with the recipient of the data, whether the law of the third country of destination ensures adequate protection, under EU law, of personal data transferred pursuant to standard data protection clauses, by providing, where necessary, additional safeguards to those offered by those clauses."

The concept that a data exporter has to assess and continuously monitor whether data importers can and do comply with their contractual obligations to protect personal data is not entirely new. According to Clause I(b) of the SCC 2004 (controllers), the data exporter in the EU must use "reasonable efforts to determine that the data importer is able to satisfy its legal obligations." According to Clause 4(c)-(e) of the SCC 2010 (processors), the data exporter in the EU must "warrant … that the data importer will provide sufficient guarantees," "that after assessment of the requirements of the applicable data protection law, the security measures are appropriate" and "that it will ensure compliance with the security measures."

Consequently, companies in the EU that have relied on SCC for cross-border data transfers have always had a duty to determine whether the data importer can and will comply with the SCC. Moreover, controllers have to conduct due diligence assessments also when they engage processors within the EU: The "controller shall use only processors providing sufficient guarantees to implement appropriate technical and organizational measures" pursuant to Article 28 EU General Data Protection Regulation. Pursuant to Article 5(2) of the GDPR, the controller must document that they diligently select and supervise processors within and outside the EU.

Extra scrutiny ex-EU

Even though due diligence duties are not new, due to the heavy emphasis that the CJEU places on the impact of government surveillance and privacy law frameworks in other countries, companies in the EU may perceive a significant increase in compliance burdens associated with cross-border data transfers.

Realistically, few companies in the EU or elsewhere have sufficient resources to competently assess other countries' data protection law regimes, surveillance practices or compliance realities. Local or national data protection authorities are also hardly in a position to provide helpful information or guidance when even the European Commission struggles with such assessments: The European Commission's current list (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en) of "adequate" jurisdictions contains a seemingly random selection of only 12 countries after more than 25 years of assessments, and the CJEU has invalided the commission's adequacy decision regarding the U.S. twice in five years. In fact, the CJEU itself only addresses a few provisions of U.S. law, does not even begin to

Union can meet (for more information on war and peace in cyberspace (http://repository.uchastings.edu)).

Consequently, companies in the EU will inevitably feel an increased pressure to keep personal data within "Fortress Europe" (or, more specifically, within the — shrinking — EU) and may have to brace for further disruptions if governments in the U.S. and other countries retaliate with trade protectionism of their own, despite the generally positive potential of knowledge- and information-sharing (http://www3.weforum.org/docs/WEF_A_Roadmap_for_Cross_Border_Data_Flows_2020.pdf) for economies and societies.

Proactive, practical steps

What can TMT service providers do?

At a minimum, providers must offer the contractual safeguards their customers need to buy and use their services in compliance with applicable law. According to the GDPR, this means unmodified SCC and national data protection laws pile on requirements in some countries.

TMT service providers can also help their customers shoulder compliance burdens by presenting an EU-based contracting entity so that the customer transfers data within the EU and the provider takes on the cross-border data transfer challenge. An EU-based provider may benefit in certain cases from the "one stop shop" treatment under Article 56 of the GDPR, which may become a critical advantage if data protection authorities across the EU form divergent views regarding the legality of cross-border transfers.

To some TMT providers, they can support research, public debates and the publication of comparative studies on national surveillance programs and privacy laws to help governments, DPAs and companies form objective views on the relative strengths of civil rights protections and threats (read examples of existing comparisons here (https://globaltmt.bakermckenzie.com/surveillance-law-comparison-guide/)). Trade associations, privacy advocates, law firms, universities, research institutions and other non-governmental organizations can play an important role, too, and, in a few years, more competent and objective assessments may emerge.

More immediately, providers can prepare informative briefings, FAQ and contractual representations to help customers in the EU get comfortable with the relative risk and meet their documentation obligations under Article 5(2) of the GDPR. Good data protection standards and documentation have already become a competitive differentiator, and the impact of "Schrems II" will likely raise the significance of a provider's efforts in this respect.

Providers in many industry sectors can proactively substantiate that they are hardly the focus of government surveillance (e.g., medical devices, pharma, manufacturing). Cloud providers (https://iapp.org/news/a/2012-03-01-data-privacy-in-the-clouda-dozen-myths-and-facts/) can show that their customers are much more likely directly exposed to government demands in their home jurisdictions than to indirect threats on their vendors. Companies in the U.S. can update companies and authorities in the EU on legislative developments in California and other states that have significantly expanded privacy laws and should qualify as more than adequate (https://doi.org/10.1093/idpl/ipw011).

Customers and prospects can also take comfort — and reference in their own internal data transfer assessments — if providers publish transparency reports regarding government access requests, publicly commit to resisting access requests court orders and actually challenge authorities in courts.

At the same time, companies in the EU have to acknowledge limitations that companies face universally: If government authorities compel access to data for national security or law enforcement purposes based on applicable law from a company within their jurisdiction, the company typically has to comply. If a government authority demands in accordance with applicable law that an investigation remains confidential, the company has

will likely be counterproductive and may result in unenforceable contracts.

Therefore, providers and users of data processing services should make good faith efforts to examine and understand each others' legal situations and work on realistic and practical arrangements that allow both sides to comply with applicable laws.

Photo by ThisisEngineering RAEng on Unsplash

iapp CPE credits approved Approved CIPM, CIPP/A, CIPP/C, CIPP/E, CIPP/G, CIPP/US, CIPT Credits: 1

SUBMIT FOR CPES (/CERTIFY/CPE-SUBMIT/)

Pease International Tradeport, 75 Rochester Ave.
Portsmouth, NH 03801 USA • +1 603.427.9200

/