WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

WEBINAR

Recent Developments of the European Framework for International Data Flows and the Impact on Businesses

JUNE 29, 2021

Speakers: Martin Braun, Kirk Nahra, Fred Louis and Shannon Togawa Mercer

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A feature
- Questions will be answered as time permits
- Offering 1 CLE credit in California and New York*
- The webcast is being streamed through your computer, so there is no dial-in number. For the best quality, please make sure your volume is up and other applications are closed. If you experience a delay or get disconnected, press F5 to refresh your screen at any time
- For additional help with common technical issues, click on the question mark icon at the bottom of your screen

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale has been approved as a Colorado Certified Provider, as recognized by the Colorado Supreme Court Continuing Legal and Judicial Education Committee. We will apply for Colorado CLE if requested. The type and amount of credit awarded will be determined solely by the Colorado Supreme Court. New Jersey grants reciprocal credit for programs that are approved in New York. We can also issue Connecticut credit for this program. All attendees, regardless of jurisdiction, will receive a uniform certificate of attendance that shows the states in which the program was approved. Attendees requesting CLE credit must attend the entire program. CLE credit is not available for on-demand webinar recordings.

WEBINAR

Speakers

Martin Braun
Partner
Co-Chair, Big Data Practice
WilmerHale

Kirk J. Nahra
Partner
Co-Chair, Big Data Practice
Co-Chair, Cybersecurity and Privacy Practice
WilmerHale

Fred Louis
Partner
WilmerHale

Shannon Togawa Mercer
Senior Associate
WilmerHale

Agenda

- New Standard Contractual Clauses
  - Structure and new elements
  - Implementation: Timelines and practical steps for companies
- EDPB Updated Recommendations and Their Impact
- Enforcement in Europe
- U.S. Businesses and Successor to Privacy Shield

New Standard Contractual Clauses

Standard Contractual Clauses – Schrems II Context

- Under GDPR, transfers from the EU/EEA to recipients outside the EU/EEA are subject to restrictions
- The so-called Standard Contractual Clauses ("SCCs") have been the most widely used option to address this requirement (by far)
- The existing SCCs were outdated because they don't address all GDPR requirements and don't use the GDPR terminology
- On July 16, 2020, the CJEU released its decision in *Schrems II*
  - Invalidation of EU-U.S. Privacy Shield
  - Upheld SCCs, but added requirements to verify or assess adequate (essentially equivalent) level of protection and make sure SCCs are effective
  - Despite the focus on the U.S., the CJEU decision applies to all transfers to countries outside the EU/EEA

Standard Contractual Clauses

- Following consultations, on June 4, 2021, the European Commission adopted and published a new set of SCCs. The decision was published in the Official Journal of the EU on June 7, 2021
- The fundamental mechanism is identical to the old SCCs: Using the SCCs without modifications addresses the GDPR requirements for international transfers of personal data
- *But* there may still be a need to take supplementary measures to ensure conformity with EU data-protection standards
- A parallel decision of the same day addresses inner-EU/EEA controller-processor transfers (Article 28 GDPR)

SCCs– Key Changes

- "Modular" SCCs now cover four different situations in one document:
  - Module 1: **controller** in the EU/EEA to **controller** outside the EU/EEA
  - Module 2: **controller** in the EU/EEA to **processor** outside the EU/EEA
  - Module 3: **processor** in the EU/EEA to **processor** outside the EU/EEA
  - Module 4: **processor** in the EU/EEA to **controller** outside the EU/EEA
- "Docking" clause permits data importers/exporters to accede to SSCs they are not party to and for multiparty contracts (Clause 7)
- Clarifies the supervisory authority for data exporters subject to the GDPR but outside the EU/EEA (Clause 13)

SCCs – Dealing with local laws in the receiving country (1)

- Clause 13:

  "The Parties warrant

  - that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer
  - including any requirements to disclose personal data or measures authorizing access by public authorities
  - prevent the data importer from fulfilling its obligations under these Clauses

  This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of the GDPR, are not in contradiction with these Clauses."

SCCs – Dealing with local laws in the receiving country (2)

- Data importer warrants that it has made best efforts to provide the data exporter with relevant information.
- Assessment must be documented and be made available to regulators upon request.
- Ongoing cooperation obligations of the exporter and the importer.
- Data importers must notify exporters and data subjects of disclosure of or granting access to personal data to public authorities.
  - If public authority prohibits notification, must use best efforts to obtain waiver.

Open Questions

- Definition of “transfer”
- Transfers already subject to GDPR, e.g., because of Article 3(2) GDPR
- Level of detail of the Transfer Impact Assessments
- Possibilities to modify liability provisions in the new SCCs
- Relevance of enforcement by data subjects in practice
- Need for supplementary measures in addition to SCCs

Implementing the New SCCs (1)

- New SCCs decision is effective June 27, 2021
- Old SCCs can be entered into until September 27, 2021
- Existing contracts using the old SCCs can continue to be relied upon until December 27, 2022 – provided the processing operations remain unchanged and the reliance on those clauses ensures that the transfer of personal data is subject to appropriate safeguards

Implementing the New SCCs (2)

- Understand existing data transfer / contractual relationships that rely on old SCCs
- Decision regarding relevant SCCs document(s)
- Prepare additional documentation, especially Transfer Impact Assessment
- Update standard agreements vs. waiting for standard documents of large (cloud) providers
- Internal transfers vs. external transfers
- For companies outside of the EU/EEA – note and plan for new requirements and obligations

EDPB Updated Recommendations and Their Impact

EDPB Updated Recommendations

- Updated Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data were published on June 21, 2021
  - Initial version was released in November 2020, followed by consultation phase
  - Retain the six-step framework for assessing transfers but makes a few important changes and clarifications
  - Intention to provide data exporters, or the parties sending personal data out of the EU to third countries, with a set of steps to help with the "complex task of assessing third countries and identifying appropriate supplementary measures where needed."
  - EDPB view: "Recommendations" apply in addition to requirements in SCCs

EDPB Updated Recommendations

- Recommendations now allow for a (limited) more subjective or risk-based approach to assessments of third-country legal regimes and data protection standards
  - Allows for consideration of third-country *practices* in addition to *laws*, if such an assessment is rigorous and documented
  - Recognizes the difference between “the law on the books” and “the law in action”
  - Assessment must also consider the experiences of other organizations engaging in similar processing activities
- Two scenarios in which, according to the EDPB, no safeguards can make transfers to countries with problematic laws legal remain:
  - importer is cloud service provider and needs access to data in the clear; or
  - importer is pursuing a shared business purpose and needs access to data in the clear

Enforcement in Europe

Status of enforcement in Europe (1)

- March 2021: Bavarian DPA and Mailchimp – prime case study
  - Mailchimp's servers in the U.S.
  - Previously certified under EU-U.S. Privacy Shield
  - Pivoted to alternative transfer mechanism following *Schrems II* (SCCs)
  - Had allegedly not examined whether additional measures were necessary
  - May be subject to data access by US intelligence services under FISA 702 as an Electronic Communications Service Provider
  - No formal decision, because German Mailchimp customer stopped using Mailchimp

Status of enforcement in Europe (2)

- April 2021: Portugal DPA ordered National Institute of Statistics to stop sending data to U.S. using Cloudflare
- German DPAs have initiated coordinated investigations
- EDPS has launched investigations into EU institutions' use of AWS, Microsoft, Microsoft 365
- Following a court decision, continued investigation by the Irish DPC regarding Facebook's post-*Schrems II* data transfers. In fall 2021, the Irish DPC had communicated its intention to prohibit these transfers.
- Recent (high-level) CNIL guidance in France
- Escalating fine pressure

U.S. Businesses and Successor to Privacy Shield

What U.S. Businesses Should Consider

- Timely compliance with (and attention to) EU requirements, when possible
- Preparation for continued, and likely more aggressive, questioning related to U.S. law generally, Transfer Impact Assessments and SCCs efficacy
- Sensitivity to EU customer (data exporter) concerns
- Supplementary measures and data localization options
- Use of SCCs Option 3 – Processor in the EU, (sub-)processor outside the EU/EEA – possible advantages from a liability perspective

EU – U.S. Negotiations

- Negotiations between the U.S. Department of Commerce and the European Commission continue
- U.S. Chamber of Commerce continuing to urge EU and U.S. to adopt successor Privacy Shield
- Some suggestions that solution could be reached before the end of the year
- June 15, 2021 summit
- Big problems remain: independent oversight and redress in relation to surveillance

Summary

- Plan for use and integration of new SCCs: consider timing carefully
- Transfer Impact Assessments may now include a (limited) more subjective, risk-based approach to assessments of third-country legal regimes and data protection standards
- Scrutiny of transfers is not just about the U.S., even though immediate focus is on the U.S.
  - Companies should think ahead to global enforcement (i.e., transfers from EEA to China, India, etc.)
- Review and investigations of data transfers have already started, and they will escalate in earnest after the summer
- A new EU-U.S. Privacy Shield may not be right around the corner

Questions

Martin Braun
Partner, Co-Chair, Big Data Practice
WilmerHale
martin.braun@wilmerhale.com

Kirk J. Nahra
Partner
Co-Chair, Big Data Practice
Co-Chair, Cybersecurity and Privacy Practice
WilmerHale
kirk.nahra@wilmerhale.com

Fred Louis
Partner
WilmerHale
frederic.louis@wilmerhale.com

Shannon Togawa Mercer
Senior Associate
WilmerHale
shannon.mercer@wilmerhale.com

@WHCyberPrivacy