WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

WEBINAR

Implementing Schrems II – The Current State of Play

MARCH 3, 2021

Speakers: Martin Braun, Frédéric Louis, 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.

Speakers

Dr. Martin Braun
Partner; Co-Chair, Big Data Practice
WilmerHale

Frédéric Louis
Partner
WilmerHale

Shannon Togawa Mercer
Senior Associate
WilmerHale

Agenda

- Background: The *Schrems II* ruling
- Subsequent developments and guidance
- Practical impact and strategies for implementing the judgment
- What to look out for

Background: The Schrems II judgment

Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems

- Following a reference by the Irish High Court, on July 16, 2020, the Court of Justice of the European Union issued its judgment in case C-311/18 (“Schrems II”)
- The judgment:
  - Declared the European Commission decision regarding the EU-U.S. Privacy Shield Framework invalid
  - Declared the European Commission decision regarding Standard Contractual Clauses (“SCC”) as valid
  - But: Introduced significant uncertainty around the details of international data transfers

Schrems II, Standard Contractual Clauses

(#133) “It follows that the standard data protection clauses adopted by the Commission on the basis of Article 46(2)(c) of the GDPR are solely intended to provide contractual guarantees that apply uniformly in all third countries to controllers and processors established in the European Union and, consequently, independently of the level of protection guaranteed in each third country. In so far as those standard data protection clauses cannot, having regard to their very nature, provide guarantees beyond a contractual obligation to ensure compliance with the level of protection required under EU law, **they may require, depending on the prevailing position in a particular third country, the adoption of supplementary measures by the controller in order to ensure compliance with that level of protection**.”

- Controller verification, on a case-by-case basis, that the law in the third country ensures adequate protection
- Additional or supplemental measures
- Data protection authorities must act to stop transfers that do not have a legal basis

EU-U.S. Privacy Shield Framework

- Primary reasons for declaring the European Commission decision regarding Privacy Shield invalid:
  - Surveillance law framework: FISA 702, EO 12333
  - Lack of effective remedies / judicial redress
- On September 8, 2020, the Federal Data Protection and Information Commissioner (FDPIC) of Switzerland issued an opinion concluding that the Swiss-U.S. Privacy Shield Framework does not provide an adequate level of protection for data transfers from Switzerland to the United States pursuant to Switzerland's Federal Act on Data Protection (FADP).
- https://www.privacyshield.gov/ continues to be online:
  - "The U.S. Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List. If you have questions, please contact the European Commission, the appropriate European national data protection authority or legal counsel."

Consequences of the Schrems II judgment

- **Privacy Shield** is no longer available as a legal basis for transfers of personal data
- The other existing **adequacy decisions** are not affected (Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland and Uruguay)
- Article 46 GDPR mechanisms can be used (with the described complications), especially
  - **SCC**
  - Binding Corporate Rules ("**BCR**")
- Article 49 GDPR (**Derogations**) is also available

Subsequent developments and guidance

November 2020: EDPB Recommendations

- On November 11, 2020, the European Data Protection Board ("EDPB") issued Recommendations on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data (Recommendations 01/2020)
  - Consultation until December 21, 2020
  - 178 submissions (published on the EDPB website)
- Accompanied by the European Essential Guarantees for surveillance measures (Recommendations 02/2021)

Content of EDPB Recommendations

Step-by-step process to help exporters assess third countries and identify appropriate supplementary measures where needed

- **Step One:** “Know your transfers”
- **Step Two:** “Verify the transfer tool your transfer relies on”
- **Step Three:** “Assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer”
- **Step Four:** “Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence”
- **Step Five:** “Take any formal procedural steps the adoption of your supplementary measure may require”
- **Step Six:** “Re-evaluate at appropriate intervals the level of protection afforded to the data you transfer to third countries and monitor if there have been or will be any developments that may affect it”

Content of EDPB Recommendations

EU Essential Guarantees (see Step 3)

- Four factors for the assessment of the "level of interference with the fundamental rights to privacy and to data protection"
  - Processing should be based on clear, precise and accessible rules
  - Necessity and proportionality with regard to the legitimate objectives pursued need to be demonstrated
  - An independent oversight mechanism should exist
  - Effective remedies need to be available to the individual

Contents of EDPB Recommendations – Measures

- **Technical Measures**
  - Encryption in transit, encryption at rest
  - Pseudonymization
- **[Contractual Measures]**
  - Assistance obligations
  - Audit rights
  - Notification of inability to comply
  - Warrant canary clauses
- **[Organizational Measures]**
  - Data security certifications
  - Data protection notices
  - Internal policies
  - Training

Contents of EDPB Recommendations – Use Cases

- **Effective**
  - **Use Case 1:** Data storage for backup and other purposes that do not require access to data in the clear
  - **Use Case 2:** Transfer of pseudonymized data
  - **Use Case 3**: Encrypted data merely transiting third countries
  - **Use Case 4**: Protected recipient
  - **Use Case 5:** Split or multi-party processing
- **Not Effective**
  - **Use Case 6:** Transfer to cloud services providers or other processors which require access to data in the clear
  - **Use Case 7:** Remote access to data for business purposes

November 2020: Draft EC Standard Contractual Clauses

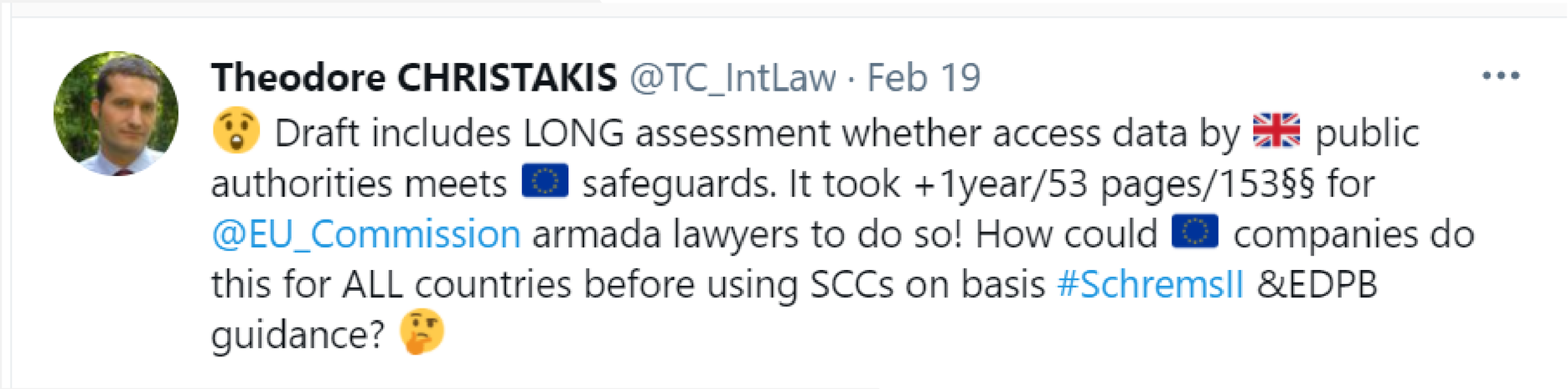
- November 12, 2020, draft Implementing Decision (data processing SCCs and SCCs for international transfers)
- Modernize and update old SCCs in light of new technology, the GDPR, and the digital economy
- Modular approach: general clauses + four modules:
  - Controller-to-controller transfers
  - Controller-to-processor transfers
  - Processor-to-processor transfers
  - Processor-to-controller transfers
- Multiple parties may adhere and accede
- Third-party beneficiary rights
- Liability and indemnification
- Open to case-specific assessment

Draft EC Standard Contractual Clauses (cont.)

- January 14, 2021, EDBP and EDPS joint opinion (2/2021)
  - Note that supplementary measures may still be necessary.
  - Suggest clarification on a number of items, including the “docking” clause and a “white-list” of the third-party beneficiary rights.
  - Further, there is a suggestion that an annex be added to capture the assessment of the third country assessment.
  - Calls for more precision in the Annexes.
- Adoption process
  - EU Member State vote
  - Anticipated mid-2021, with a one-year transition period
- Not a cure-all for *Schrems II* complications

February 2021: Draft Adequacy Decision for UK

- On February 18, 2021, the European Commission published its draft adequacy decision in respect of the United Kingdom.
- If adopted, the UK would be granted adequacy for four years following its entry into force



Practical impact and strategies for implementation

Impact of Schrems II and EDPB Guidance

- Under current EDPB guidance, all transfers of personal data
  - to processors outside the EEA with access to the data
  - to recipients who can see the data generally already seem problematic
  - Significant uncertainty regarding legality of transfers from the EEA to the U.S.
- Under current EDPB guidance
  - “supplementary measures” must be of technical nature
  - no risk-based approach
- Risk of complaints, supervisory authority investigations and activist litigation

Strategies for Implementation – Privacy Shield

- No transfers based on Privacy Shield
  - No tolerance by supervisory authorities for continued reliance
  - Changing to Standard Contractual Clauses typically does not require negotiations
  - Identification of all relevant transfers

Strategies for Implementation – Derogations

- EDPB has stated that its Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 continue to apply
  - Use of consent
  - Use of contractual necessity
  - Other
- Comments by Judge Thomas von Danwitz on January 28, 2021, regarding use of Article 49 GDPR

Strategies for Implementation – Binding Corporate Rules

- The EDPB has continued to approve BCRs
- Consensus that Schrems II also applies to BCRs
- Latest EDPB statement (February 16, 2021):

  "10. In accordance with the judgment of the Court of Justice of the European Union C-311/1876, it is the **responsibility of the data exporte**r in a Member State, if needed with the help of the data importer, **to assess** whether the level of protection required by EU law is respected in the third country concerned, in order to determine **if the guarantees provided by BCRs can be complied with in practice**, taking into consideration the possible interference created by the third country legislation with the fundamental rights. If this is not the case, the data exporter in a Member State, if needed with the help of the data importer, should assess whether they can provide **supplementary measures** to ensure an essentially equivalent level of protection as provided in the EU."

Strategies for Implementation – Standard Contractual Clauses

- Follow the steps in the EDPB recommendations and implement supplementary measures if and when necessary
- Document all compliance steps, assessments, and decisions
- Engage with your data exporters and data importers to pursue a collaborative approach to *Schrems II* compliance
- Consider options for data localization in the EEA and the extent of possible benefits
- Internal guidance for sourcing department (?)
- Legal opinions regarding the laws of specific countries (?)
- Use of vendor questionnaires (?)
- Standardized separate transfer impact assessments (?)

Strategies for Implementation – Standard Contractual Clauses

If you are a data importer in the U.S.

- If your organization was certified under Privacy Shield, do not forget that the U.S. Privacy Shield program is still being administered and obligations may be enforced
  - If you are currently registered, consider the costs and benefits of renewal
- Review your privacy policies and other external representations to guarantee that disclosures about data transfers are up to date
- Prepare for questions from partners in the EEA, including due diligence questionnaires
  - These questions may address exposure to U.S. authority surveillance, the U.S. surveillance legal landscape generally, and/or your company's technical and organizational measures in place for the security of personal data in transit and at rest
- Prepare for potential negotiation with EEA data exporters concerning supplementary contract clauses
- Consider options for data localization in the EEA (data center, support staff) and the extent of possible benefits
  - Prepare for discussions with partners in the EEA concerning data localization options

Backup: Content of EDPB Recommendations

Step-by-step process to help exporters assess third countries and identify appropriate supplementary measures where needed

- **Step One:** “Know your transfers”
- **Step Two:** “Verify the transfer tool your transfer relies on”
- **Step Three:** “Assess if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the transfer tools you are relying on, in the context of your specific transfer”
- **Step Four:** “Identify and adopt supplementary measures that are necessary to bring the level of protection of the data transferred up to the EU standard of essential equivalence”
- **Step Five:** “Take any formal procedural steps the adoption of your supplementary measure may require”
- **Step Six:** “Re-evaluate at appropriate intervals the level of protection afforded to the data you transfer to third countries and monitor if there have been or will be any developments that may affect it”

What to look out for

What To Look Out For

- Supervisory authorities continue to work on Schrems August 2021 complaint (Google Analytics, Facebook Connect) and other complaints
- Irish court case regarding Facebook data transfers continues
- German authorities will start sending out questionnaires to randomly chosen companies in the coming weeks
- German authorities will continue investigating video conferencing solutions and Microsoft Office 365.
- Continued interest in U.S. headquartered cloud services providers

What To Look Out For (cont.)

- Updated Standard Contractual Clauses
- UK adequacy decision
- Updated Recommendations 01/2020
- EU-U.S. successor to Privacy Shield
  - Negotiations are ongoing
  - Christopher Hoff, deputy assistant secretary for services at the U.S. Department of Commerce is the European Commission's primary interlocutor in the discussions.
- Developments in U.S. law

Contact

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

Frédéric Louis
Partner
WilmerHale
frederic.louis@wilmerhale.com

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

WilmerHale Privacy and Cybersecurity Law Blog

Twitter: @WHCyberPrivacy