WILMERHALE

WILMER CUTLER PICKERING HALE AND DORR LLP ®

WEBINAR

International Data Flows Following the Schrems II Ruling of the Court of Justice of the European Union

JULY 20, 2020

Speaker: Dr. Martin Braun

Attorney Advertising

WEBINAR

Speaker

Dr. Martin Braun
Partner, Co-Chair of Big Data Practice
WilmerHale Frankfurt/Brussels

+49 27 107 8019 | +49 160 96346912
martin.braun@wilmerhale.com

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.

Agenda

- The Judgment
- Background
- Reasoning of the Court, Comments
- Consequences
- Q&A

The Judgment

CJEU, C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems (July 16, 2020)

- Privacy Shield: The decision of the European Commission on the adequacy of the protection awarded by the EU-US Privacy Shield is **invalid** (without grace period).

- Standard Contractual Clauses. The decision of the European Commission on standard contractual clauses for the transfer of personal data to processors established in third countries is **valid**.
  Transfers based on standard data protection clauses must be subject to **appropriate safeguards, enforceable rights and effective legal remedies** that afford data subjects whose personal data are transferred to a third country a **level of protection that is essentially equivalent to that guaranteed within the EU** by the GDPR (read in the light of the Charter of Fundamental Rights of the EU).

Background

Background – European Data Protection Law Framework for International Data Transfers

- The EU General Data Protection Regulation ("GDPR") has replaced Directive 95/46/EC on May 25, 2018.
- Cross-border flows of personal data within the European Union and the EEA (Iceland, Liechtenstein, Norway) are not subject to restrictions.
- Additional requirements for transfers so so-called "Third Countries".
- Mechanisms to address the additional requirements:
  - Adequacy decision by the European Commission, Article 45 GDPR.
  - Appropriate safeguards, Article 46 GDPR
    - Standard data protection clauses (formerly: "Standard contractual clauses")
      - Controller to controller (2001 and 2004 versions)
      - Controller to processor (2010)
    - Binding Corporate Rules, Article 46(2)(b), Article 47 GDPR
  - Exceptions, Article 49 GDPR

Background – Complaint/Litigation in Ireland

- **2013**: Schrems complaint to Irish data protection authority regarding Facebook data transfers to the U.S.
- 2015: Update of the complaint in light of the Safe Harbor judgment – Focus on “Standard Contractual Clauses” mechanism.
- Lawsuit brought by the Irish Data Protection Commissioner against Facebook Ireland Limited and Maximilian Schrems. Amici curiae: United States of America, the Business Software Alliance (BSA), Digital Europe and the Electronic Privacy Information Centre (EPIC).
- **3 October 2017**
  Judgment of the High Court; Referral to the CJEU. Focus: transfer of personal data for commercial purposes, but further processed for national security and law enforcement purposes in the third country.
- 13 April 2018
  Decision on the questions to be referred to the CJEU: Validity of the the 2010 Standard Contractual Clauses, but Privacy Shield is mentioned.

Background – CJEU, Schrems II

- Oral hearing on 9 July 2019

- Opinion of the Advocate General on **19 December 2019**:

> "343. I propose that the Court answer the questions for a preliminary ruling referred by the High Court, Ireland, as follows:
>
> Analysis of the questions for a preliminary ruling has disclosed nothing to affect the validity of Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016."

- Parallel proceedings: Case T-738/16 – *La Quadrature du Net and Others v Commission*: Oral hearing was planned (July 2019), but cancelled.

Reasoning of the Court, Comments

Reasoning of the Court

- The referral was submitted before May 25, 2018, but the questions of the Irish High Court must be answered in the light of the provisions of the GDPR rather than those of Directive 95/46.
- Article 2(1) and (2) GDPR must be interpreted as meaning that the GDPR applies to the transfer of personal data for commercial purposes by an economic operator established in a Member State to another economic operator established in a third country, irrespective of whether, at the time of that transfer or thereafter, that data is liable to be processed by the authorities of the third country in question for the purposes of public security, defense and State security.

(#79-89)

Comments

- Article 2 GDPR (Material scope) is discussed:
  - The court mentions Art. 4(2) TFEU, according to which, within the EU, national security remains the sole responsibility of each Member State. It clarifies that this concerns Member States only.
  - The act of transferring personal data from a Member State to a third country constitutes, in itself, processing of personal data within the meaning of Article 4(2) GDPR, carried out in a Member State, and falls within the scope of the GDPR under Article 2(1) GDPR.
  - Exclusions in Article 2(2) GDPR do not apply.

- No discussion of Article 3 GDPR (Territorial scope).
- Definition of “transfer” is not discussed.

Reasoning of the Court

- Article 46(1) and Article 46(2)(c) GDPR must be interpreted as meaning that the **appropriate safeguards, enforceable rights and effective legal remedies** required by those provisions must ensure that data subjects whose personal data are transferred to a third country pursuant to standard data protection clauses are afforded **a level of protection essentially equivalent to that guaranteed within the EU by the GDPR**, read in the light of the Charter of Fundamental Rights of the EU.
- To that end, the assessment of the level of protection afforded in the context of such a transfer must, in particular, **take into consideration both the contractual clauses** agreed between the controller or processor established in the EU and the recipient of the transfer established in the third country concerned **and**, as regards any access by the public authorities of that third country to the personal data transferred, **the relevant aspects of the legal system of that third country, in particular those set out, in a non-exhaustive manner, in Article 45(2) of that regulation**.

(#90-105)

Article 45(2) GDPR

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

a) the **rule of law**, **respect for human rights and fundamental freedoms**, **relevant legislation**, both general and sectoral, including concerning public security, defense, national security and criminal law and the access of public authorities to personal data, as well as the **implementation of such legislation**, data protection rules, professional rules and security measures, including rules for the onward transfer of personal data to another third country or international organization which are complied with in that country or international organization, **case-law**, as well as **effective and enforceable data subject rights** and **effective administrative and judicial redress for the data subjects whose personal data are being transferred**;

b) the existence and effective functioning of one or more **independent supervisory authorities** in the third country or to which an international organization is subject, with responsibility for ensuring and enforcing compliance with the data protection rules, including **adequate enforcement powers**, for assisting and advising the data subjects in exercising their rights and for cooperation with the supervisory authorities of the Member States; and

c) the **international commitments** the third country or international organization concerned has entered into, or other obligations arising from legally binding conventions or instruments as well as from its participation in multilateral or regional systems, in particular in relation to the protection of personal data.

Comments

- The court relies on Article 44 GDPR to require a high standard for data transfers based on standard data protection clauses.
- Article 46 GDPR requires
  - appropriate safeguards (e.g. standard data protection clauses), and
  - the availability of enforceable data subject rights and effective legal remedies for data subjects. “All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by the GDPR is not undermined.” (Article 44 GDPR)
- Controllers relying on standard data protection clauses are apparently required to conduct an analysis that is very similar to the analysis of the European Commission prior to an adequacy decision.
- An “**adequate level of protection**” must be ensured, and understood as requiring a level of protection of fundamental rights and freedoms that is “**essentially equivalent**” to that guaranteed in the EU. Details: Article 45(2) GDPR (not exhaustive).

Reasoning of the Court

- Article 58(2)(f) and (j) GDPR must be interpreted as meaning that, **unless there is a valid European Commission adequacy decision**, **the competent supervisory authority is required to suspend or prohibit a transfer of data to a third country pursuant to standard data protection clauses** adopted by the Commission, if, in the view of that supervisory authority and in the light of all the circumstances of that transfer, those clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law, in particular by Articles 45 and 46 GDPR and by the Charter of Fundamental Rights, cannot be ensured by other means, **where the controller or a processor has not itself suspended or put an end to the transfer**.

(#106-121)

Comments

- Each DPA is vested with the power to check whether a transfer of personal data complies with the requirements in the GDPR.
- Each DPA is required on its territory to handle complaints, and to examine the nature of that complaint as necessary. DPA must act where such action is necessary to protect the rights of the data subject.
- DPA is obliged to suspend or prohibit a transfer of personal data to a third country if, in its view, the standard data protection clauses are not or cannot be complied with in that third country and the protection of the data transferred that is required by EU law cannot be ensured by other means, where the controller or a processor has not itself suspended or put an end to the transfer.
- Adequacy decisions are binding until declared invalid by the CJEU. If a DPA has doubts regarding the validity, it must bring this question before a national court, which can then refer the matter to the CJEU.

Reasoning of the Court

- Examination of Commission Decision 2010/87/EU of 5 February 2010 on **standard contractual clauses** for the transfer of personal data to processors established in third countries under Directive 95/46/EU, as amended by Commission Implementing Decision (EU) 2016/2297 of 16 December 2016 in the light of Articles 7, 8 and 47 of the Charter of Fundamental Rights has **disclosed nothing to affect the validity of that decision**.

(#122-149)

Comments

- SCC are not binding on authorities in Third Countries.
- SCC are just general language, that do not take into consideration the specific situation in a specific Third Country. In some countries, this might be sufficient. Where the law of the receiving country allows its public authorities to interfere with the rights of data subjects, the content of the standard clauses does not a sufficient means of ensuring, in practice, the effective protection of personal data transferred to the third country concerned. (#126)
- Requirement to adopt “supplementary measures” (#133), “additional safeguards” (#134), “effective mechanisms”. (#137)
- Controller or processor must 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 ensures adequate protection.
- Recipient must inform the exporter of inability to comply with the standard data protection clauses, even if the recipient is not obliged to disclose the specific request by law enforcement, Clause 5(d)(i).
- Breach of standard data protection clauses may lead to damage claims, Clause 6.

Reasoning of the Court

- Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC on the adequacy of the protection provided by the EU-US Privacy Shield is **invalid**.
- In view of Article 49 GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create a legal vacuum. That article details the conditions under which transfers of personal data to third countries may take place in the absence of an adequacy decision under Article 45(3) GDPR or appropriate safeguards under Article 46 GDPR.

(#150-202)

Comments

- Clarification that the adherence to the principles may be limited, inter alia, to the extent necessary to meet national security, public interest, or law enforcement requirements is problematic from a GDPR perspective.
- Section 702 of the FISA and E.O. 12333 do not meet the requirements of Article 52 of the Charter (limitations of rights must be provided for by law, limitations must be proportionate).
- Ombudsman mechanism is not sufficient in light of requirements of Article 47 of the Charter, which requires a right to an effective remedy before a tribunal.

- This appears to be a much stricter standard than the case law of the ECHR court in Strasbourg.

- The deficiencies affect the validity of the entire decision. No grace period because of Article 49 GDPR.
- See: EDPB, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on May 25, 2018.

Consequences

Consequences – Privacy Shield

- UK ICO: “If you are currently using Privacy Shield please continue to do so until new guidance becomes available. Please do not start to use Privacy Shield during this period.”
- EDPB: “The EDPB intends to continue playing a constructive part in securing a transatlantic transfer of personal data that benefits EEA citizens and organizations and stands ready to provide the European Commission with assistance and guidance to help it build, together with the U.S., a new framework that fully complies with the EU data protection law.”
- Secretary of State Pompeo: “The United States will continue to work closely with the EU to find a mechanism to enable the essential unimpeded commercial transfer of data from the EU to the United States.”
- Commissionier Jourová: “We will be working closely with our American counterparts, based on today's ruling. Both Didier and I have been in contact with U.S. Commerce Secretary Wilbur Ross in the past days.” “Work is under way.”
- The Swiss DPA is reviewing the impact of the judgment on the Swiss-US Privacy Shield.

Consequences – Standard Data Protection Clauses

- The European Commission has already prepared updated versions of the standard data protection clauses. These will be published in the near future.
- Irish DPC: “The CJEU has also ruled that the SCCs transfer mechanism used to transfer data to countries worldwide is, in principle, valid, although it is clear that, in practice, the application of the SCCs transfer mechanism to transfers of personal data to the United States is now questionable. This is an issue that will require further and careful examination, not least because **assessments will need to be made on a case by case basis**.”
- EDPB: “[…] If the result of this assessment is that the country of the importer does not provide an essentially equivalent level of protection, the exporter may have to consider putting in place additional measures to those included in the SCCs. **The EDPB is looking further into what these additional measures could consist of.**”

Consequences – Binding Corporate Rules

- Not directly addressed in the CJEU judgment.
- General observations regarding Article 46 GDPR also apply to Binding Corporate Rules.
- Initial DPA statements were very cautious regarding BCRs.

Consequences – European Commission Adequacy Decisions

- The European Commission is currently reviewing its existing adequacy decisions. Increased pressure regarding “Five Eyes” countries (Australia, Canada, New Zealand) seems likely. Israel could also be subject to additional scrutiny.
- There is also a pipeline of additional adequacy decisions, e.g. regarding Korea.
- A possible adequacy decision for the United Kingdom likely became more difficult. The UK is also part of the “Five Eyes” group of countries.

Consequences – Data Protection Authorities

- The judgment mentions the EDPB, its coordination role, and the option to adopt decisions based on Article 64(2) GDPR (#147).
- The Berlin DPA has already requested that controllers should change to (cloud) service providers in the EU or in a country with an adequacy decision.
- Several DPAs have already mentioned China, Russia, and India.

Consequences – Data Exporters

- Identify recipients of personal data relying on Privacy Shield.
- Read the clauses, compliance with the contractual obligations is a key topic
- Criteria for assessments of recipient countries and additional measures beyond the SCC will have to be developed.
  - Access by authorities beyond what would be acceptable in the EU?
  - Gencarelli: nature of the data, volume of the data, purpose of the transfer (?)
  - Determine reach of Section 702 FISA for specific data exports.
  - Encryption is likely becoming more relevant: The CJEU mentions that data in transit may be subject to E.O. 12333 (#183)
- Increased data localization? Definition of “transfer”? Corporate reorganization?
- Re-read the guidance on Article 49 GDPR…
- Update privacy notices

Consequences – Data Importers

- Prepare documentation of laws in the country of the data importer.
- Additional education of European exporters regarding U.S. law, especially the reach of Section 702 FISA and E.O. 12333.
- Clarifications regarding the interpretation of the term “electronic communications service provider” in the meaning of Section 702 FISA.
- Replace Privacy Shield with SCC (for lack of a better option).

Questions?

WEBINAR

Speaker

Dr. Martin Braun
Partner, Co-Chair of Big Data Practice
WilmerHale Frankfurt/Brussels

+49 27 107 8019 | +49 160 96346912
martin.braun@wilmerhale.com