CMS

Law . Tax

Guide on international data transfers

Drawing on the Schrems II Case

CMS Spain

August 2020

Guide on international data transfers – Drawing on the Schrems II Case

Javier Torre de Silva, José Luis Piñar & Miguel Recio

On 16 July 2020, almost five years after the Safe Harbour Agreement between the European Union and United States was ruled invalid, the Court of Justice of the European Union (CJEU) delivered a judgment on the C-311/18 case (the Schrems II case) also invalidating the Privacy Shield adopted to replace the former Agreement.

Conversely, the CJEU has ruled that Commission Decision of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors is in fact valid.

Recognised as one of the most critical data protection rulings delivered by the CJEU in recent years, the judgment poses significant questions to those who transfer personal data outside of the European Economic Area (EEA) and for the digital economy, calling for a robust framework to be able to respond to such uncertainty.

Contents

1. Europe's new international data transfer landscape

One of the key pillars on which the General Data Protection Regulation (GDPR) is based is the guarantee to uphold the right to data protection not only in the European Union but beyond its borders when processing may affect someone within the Union. Cross-border flows of personal data (an increasingly common occurrence) "are necessary for the expansion of international trade and international cooperation", albeit the level of protection ensured by the Regulation should not be undermined, including in cases of onward transfers of personal data from the third country to another (Article 44 and Recital 101 of the GDPR). The GDPR contains complex provisions on international transfers (Articles 44 to 50)[1] which include mechanisms to ensure that the destination of the data to be transferred offers an adequate level of protection in comparison with that of the GDPR. Among such mechanisms, and in order to facilitate data transfers to the U.S., the European Union adopted the so-called Privacy Shield system (replacing the Safe Harbour Agreement), which the CJEU has recently declared invalid in its judgment delivered on 16 July 2020 (the Schrems II case C-311/18). The ruling affects thousands of companies carrying out countless data transfers on a daily basis which contain rafts of personal data. Given the immeasurable economic consequences for companies, on the same day the judgment was delivered the European Commission announced that it would work to find a swift solution to the situation created.

Moreover, the CJEU has ruled that one of the other mechanisms to protect international transfers, namely standard contractual clauses for the transfer of personal data to processors in third countries approved under Commission Decision 2010/87/EU, is valid.

According to the Spanish Data Protection Agency, the judgment marks "a turning point for the way in which data is transferred internationally to the U.S." and requires "a unified response at European level", i.e. a common approach ensuring "consistent application of the judgment across all EU countries".[2] In turn, the European Data Protection Board (EDPB) promptly issued a communiqué highlighting the need to adopt a new framework for international transfers which fully complies with European data protection regulation.[3]

CMS recognised the impact of the judgment on companies and the key concerns raised for those who transfer personal data outside of the EEA and for the digital economy from the outset,[4] as well as the need to delve deeper in order to respond to the many questions and uncertainties uncovered.

2. Schrems II case: one decision ruled invalid and another the opposite ("with reservations")

The judgment of the Court of Justice of the European Union (Grand Chamber) delivered on 16 July 2020 in case C-311/18 follows on from the ruling which invalidated the Safe Harbour Agreement[5] between the European Union and United States.

The aim of the two judgments was to respond to referrals for preliminary rulings as part of the claims filed by a Facebook user over the transfer of their personal data from Facebook Ireland (EU) to Facebook Inc. (United States). In both cases, the claims were filed by a resident of Austria to the Irish Data Protection Authority.

---

1. Please see: Piñar Mañas, José Luis, "Personal data transfers to third countries or international organisations", in Piñar Mañas, José Luis (Director), Álvarez Caro, María and Recio Gayo, Miguel (Coordinators), General Data Protection Regulation, towards a new European data protection model, Reus, Madrid, 2016; and Piñar Mañas, José Luis (Director) and Recio Gayo, Miguel (Coordinator), Data Protection Memoir, Francis Lefebvre, Madrid, 2019.

2. Spanish Data Protection Agency, "The Court of Justice of the European Union declares the Privacy Shield for international data transfers to the U.S. invalid, 22 July 2020".

3. Statement on the CJUE Judgment in Case C-311/18, 17 July 2020.

4. Schrems strikes again: EU-US Privacy Shield invalid; Standard Contractual Clauses upheld but due diligence required.

5. Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce. Invalidated by the CJEU (Grand Chamber) judgment of 6 October 2015, case C-362/14.

However, the two judgments differ in terms of the mechanisms foreseen for international data transfers; while the first judgment ruled the Decision on the Safe Harbour Agreement invalid, most notably in relation to the restrictions on exercising the powers afforded to data protection authorities, the second judgment invalidating Implementing Decision (EU) 2016/1250 of 12 July 2016 on the Privacy Shield[6] focused on data protection authorities' obligations, as well as those of controllers and processors, to ensure an adequate level of data protection.

In addition to invalidating the Implementing Decision, the CJEU also ruled on the validity of standard contractual clauses approved in view of Commission Decision 2010/87/EU[7] of 5 February 2010. Although it concludes that this Decision is valid "in light of Articles 7, 8 and 47 of the Charter of Fundamental Rights", we must take into account that the text includes obligations imposed on data controllers (exporters) and processors (importers) as key parties in ensuring the above-mentioned adequate level of protection. Against this backdrop, even where the standard clauses are valid, if the pertinent measures are not adopted, the clauses will not be enough to transfer data internationally due to a lack of sufficient guarantees. As indicated in the frequently asked questions released by the EDPB on 23 July[8], both data exporters and importers will be obliged to verify, prior to any international transfer, whether that level of protection is respected in the third country concerned. Such verification means taking into account the circumstances of the transfer, thus entailing a stringent data protection assessment.

3. Why has the CJEU invalidated the Commission's Implementing Decision (EU) 2016/1250?

The CJEU invalidated the Commission's Implementing Decision (EU) 2016/1250 due to it being incompatible with the GDPR[9], as interpreted in light of the Charter of Fundamental Rights of the European Union (CFREU).

Specifically, the CJEU found that the Commission "disregarded the requirements of Article 45(1) of the GDPR, read in light of Articles 7, 8 and 47 of the Charter" (section 198 of the C-311/18 judgment), and is therefore invalid (section 199 of C-311/18).

According to the CJEU, in Implementing Decision (EU) 2016/1250, the Commission failed to observe the requirement for the third country, in this case the U.S., to ensure an adequate level of protection.

Said adequate level of protection must be interpreted pursuant to the following fundamental rights:

— Respect for private and family life (Article 7 of the CFREU);

— Protection of personal data (Article 8 of the CFREU), and

— Right to an effective remedy and to a fair trial (Article 47 of the CFREU).

4. What does the CJEU judgment mean for transfers to the U.S.?

As of 16 July 2020, personal data can no longer be transferred to the United States under the Privacy Shield, following the CJEU ruling which declared it invalid. Since the U.S. is considered a third country lacking an adequate level of protection, the EU-based data controller or processor must refer to one of the other mechanisms set out under the GDPR in order to provide sufficient guarantees.

---

6. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield.

7. 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.

8. Available at: https://edpb.europa.eu/news/news/2020/european-data-protection-board-publishes-faq-document-cjeu-judgment-c-31118-schrems_en.

9. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

In other words, the Privacy Shield is no longer an option to transfer personal data out of the EU to a company adhering the Shield. Data transfers to the U.S. will have to be underpinned by an adequate guarantee such as standard contractual clauses, standard clauses implemented by a data protection authority and approved by the Commission, or Binding Corporate Rules (BCRs).

Should a new agreement be reached between the European Union and the United States in the future, data may be transferred to companies adhering to the programme replacing the Privacy Shield once again, which is something we cannot rule out given the interest shown on both sides of the Atlantic.

From an economic perspective, the U.S. Department of Commerce has announced that invalidating the Privacy Shield could have a devastating impact on a transatlantic relationship worth more than seven (7) trillion dollars, not to mention the European companies having to turn to other mechanisms to transfer data internationally if they wish to access the services provided by over 5,300 Privacy Shield participants[10].

5. Does the CJEU judgment completely wipe out the Privacy Shield?

Although the CJEU has invalidated the Commission's Implementing Decision (EU) 2016/1250, the Privacy Shield has not disappeared for the U.S.-based companies which adhere to it.

At this stage, it is important to bear in mind that such invalidation means that data controllers who transfer personal data from the EEA to companies adhering to the Privacy Shield are no longer able to do so using this mechanism, i.e. from 16 July 2020 all international data transfers by virtue of the Privacy Shield require further adequate guarantees.

Nevertheless, in a statement on the CJEU judgment[11], the U.S. Secretary of Commerce announced that the Department of Commerce will continue to administer the Privacy Shield programme, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List, which you can find here.

Administration of the Privacy Shield programme corresponds to the Department of Commerce under the terms of Annex I of the Commission's Implementing Decision (EU) 2016/1250.

6. Could the CJEU's ruling on the Privacy Shield case apply to third countries with a Commission adequacy decision?

The CJEU's conclusion regarding the Privacy Shield could translate to the case of other countries in terms of the requirement to ensure an adequate level of protection similar or equivalent to that of the EU. As indicated by the CJEU in its 5 October 2015 judgment invalidating the Safe Harbour Agreement, the third country is required to provide a level of protection that is "essentially equivalent to that guaranteed within the European Union" (section 73 of the C-362/14 judgment), as opposed to requiring the third country "to ensure a level of protection identical to that guaranteed in the EU legal order".

Such requirement, to be interpreted and applied in accordance with the fundamental rights set forth under the CFREU, refers to any non-EU third country or international organisation, albeit the GDPR also applies in EEA countries.

10. U.S. Secretary of Commerce Wilbur Ross Statement on Schrems II Ruling and the Importance of EU-U.S. Data Flows.

11. *Ibid.*

What's more, it is important to point out that, in contrast to the adequacy decision, the Commission's other decisions on adequate levels of protection – such as those relating to standard contractual clauses – refer to "a diverse range of privacy systems, representing different legal traditions"[12].

7. What does the CJEU judgment mean for data processors and controllers in relation to Commission Decision 2010/87/EU on standard contractual clauses?

Although the CJEU has declared Decision 2010/87/EU as valid, it is keen to remind us and emphasise the fact that controllers and processors, as well as data protection authorities, are subject to obligations under the GDPR in relation to upholding the fundamental right to data protection when transferring data internationally. In particular, the CJEU judgment states that "in the absence of an adequacy decision, a controller or processor may transfer personal data to a third country only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available" (section 128, C-311/18), which could be achieved using standard clauses. Contrary to the norm prior to the GDPR entering into force, this implies that it "may require the adoption of supplementary measures to those standard data protection clauses" (section 133, case C-311/18).

As initial steps, controllers planning to transfer data from the EEA by virtue of approved standard contractual clauses are recommended to:

i. **Verify whether the third country (non-EEA) ensures adequate protection in particular reference to governmental access to personal data when in transit or processed in the third country**. This should be done on a case-by-case basis in view of the specific circumstances and applicable legislation in the third country, as well as in collaboration with the data recipient, where necessary.

ii. As part of the above analysis, the controller must **discover whether special categories of data are being transferred** and, if so, **inform**:

   — "the data subject before, or as soon as possible after, the transfer" (section 144, case C-311/18) and

   — enable the data subject to be in a position "to bring legal action against the controller" (section 144, case C-311/18).

iii. **Notify the data protection authority of any legislative amendments applicable to the importer in the third country which have a "substantial adverse effect on the warranties and obligations provided by the standard data protection clauses"** (section 145, case C-311/18), when informed of such by the importer or recipient;

iv. Where necessary, **establish additional guarantees on top of those afforded under the standard clauses**, for example the obligation for the processor to inform and adopt measures when receiving a request from the third country government to access the personal data;

v. **Analyse or assess the enforceability of the additional guarantees** given the need to prove that the data is adequately protected;

vi. **Keep in mind the power to suspend or cancel the international transfer** – which may involve terminating an agreement – to the recipient country where adequate protection is not provided and, as the case may be, recognise that the data protection authority may order such suspension or cancellation.

---

12. European Commission (2017), Communication from the Commission to the European Parliament and the Council, Exchanging and Protecting Personal Data in a Globalised World, COM(2017) 7 final, Brussels, p. 7.

vii. It should also be taken into account that any **refusal or absence of the importer may mean that as processor they fail to offer "sufficient guarantees"**, in which case measures must be taken in view of accountability obligations, and

viii. **Consider the above implications in the case of other international transfer mechanisms**, including BCRs.

The data protection authorities are also expected to provide guidance on this as well.

Where international data transfers were already being executed:

i. **Review each international transfer** in order to verify whether they were based on the Privacy Shield:

— If so:

- **Verify whether there are any alternatives to said mechanism**, given that on occasions the processors adhering to the Privacy Shield also offered certain alternatives, or since importers may now provide solutions to the situation generated by the invalidation of the Shield;
- Where the above does not occur, **put a stop to the transfer due to a lack of adequate guarantees** when transferring data internationally, and
- In relation to the preceding point, **seek an alternative to the Privacy Shield**, i.e. another mechanism which offers adequate guarantees for the international transfer of data when there is no adequate decision in place.

In any event, given its invalidity, the Privacy Shield ceases to apply in relation to the possibility of using it as a means of implementing adequate guarantees for the international transfer of data to companies adhering to the Shield in the United States.

— In particular, bear in mind that if the international transfer fails to offer an adequate level of protection, the controller will be forced to suspend or cancel the transfer, with the data protection authority having the power to do so as well.

The analysis or assessment on whether there is an adequate level of protection in place also falls under the responsibility of the data controller acting as the exporter, which naturally has a significant impact on the data protection measures to be implemented. Said assessment is critical in the establishment of supplementary guarantees to be added to the standard contractual clauses.

In a nutshell, one of the key takeaways in this regard is that data controllers or processors who export personal data outside of the EEA – regardless of the mechanism used – will have to carry out an assessment of the data protection guarantees applied, which in turn will require specialist advice.

8. What alternatives does the GDPR provide for international data transfers?

Aside from adequacy decisions, the GDPR includes diverse set of "mechanisms that are flexible enough to adapt to a variety of different transfer situations"[13].

13. *Ibid*, p. 11.

In the case of the private sector, the adequate guarantees to be provided when transferring data to outside of the European Union are:

— Binding corporate rules (Article 46.2.b) of the GDPR).

— Standard contractual or data protection clauses adopted by a supervisory authority and approved by the Commission (Article 46.2.d) of GDPR).

— Approved codes of conduct pursuant to Article 40 of the GDPR, together with binding and enforceable commitments (Article 46.2.e) of the GDPR).

— Approved certification mechanisms pursuant to Article 42 of the GDPR, together with binding and enforceable commitments (Article 46.2.f) of the GDPR).

The Binding Corporate Rules were created as part of the Article 29 Data Protection Working Party, given that they were not foreseen under the now repealed Directive 95/46/EC, although were included in the GDPR. Regarding the possibility of using BCRs, an approval process must be followed with the leading authority when it comes to business groups present in several EU Member States. Nevertheless, as stated by the EDPB in its frequently-asked questions, the use of BCRs for international data transfers to the U.S. also requires an assessment to ensure that they comply with adequate data protection guarantees, since U.S. law will also have primacy over this tool.

In terms of standard contractual clauses, it should be noted that the CJEU has declared the above-mentioned Decision 2010/87/EU valid, notwithstanding the specific questions raised. Standard clauses adopted by a data protection authority must also be approved by the European Commission. In relation to these clauses, the EDPB has declared the assessment necessary and that where reaching the conclusion that, taking into account the circumstances of the transfer and possible supplementary measures, appropriate safeguards would not be ensured, the transfer must be suspended. However, if the intention is to keep transferring data, the relevant data protection authority must be notified.

As for codes of conduct and certification mechanisms, we will have to wait until the former are approved, given that despite being foreseen under the GDPR, they are yet to be applied to international data transfers.

Lastly, we will also have to keep a close eye on the derogations for specific situations (Article 49 of the GDPR), which will require a case-by-case analysis. These derogations only apply when there is no adequacy decision or other adequate guarantees in place and, in any event, are interpreted restrictively, as indicated by the EDPB[14].

14. European Data Protection Board, Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, adopted on 25 May 2018.

9. References

CJEU judgment and Advocate-General's conclusions:

— Judgment of the Court of Justice (Grand Chamber), 16 July 2020, case C-311/18.

— Conclusions of the Advocate-General presented on 19 December 2019.

CMS documents:

— Schrems strikes again: EU-US Privacy Shield invalid; Standard Contractual Clauses upheld but due diligence required.

Data protection authorities and other sources:

— Spanish Data Protection Agency, The Court of Justice of the European Union declares the Privacy Shield for international data transfers to the U.S. invalid, 22 July 2020.

— French Data Protection Authority (CNIL), Invalidation of the Privacy Shield: the CNIL and its counterparts are currently analysing the consequences, 17 July 2020.

— Data Protection Commission (Ireland), DPC statement on CJEU decision, 16 July 2020.

— European Data Protection Board, Thirty-fourth Plenary session: Schrems II, Interplay PSD2 and GDPR and letter to MEP Ďuriš Nicholsonová on contact tracing, interoperability of apps and DPIAs, 20 July 2020.

  - Statement on the CJEU Judgment in Case C-311/18, 17 July 2020.
  - FAQs on Schrems II.

— European Data Protection Supervisor, EDPS Statement following the Court of Justice ruling in Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximilian Schrems ("Schrems II"), 17 July 2020.

— European Commission, Opening remarks by Vice-President Jourová and Commissioner Reynders at the press point following the judgment in case C-311/18 Facebook Ireland and Schrems, 16 July 2020.

— Federal Commissioner for Data Protection and Freedom of Information (Germany), The BfD's statement on the Schrems II judgment of the ECJ, 16 July 2020.

— Information Commissioner's Office (UK), ICO statement on the judgment of the European Court of Justice in the Schrems II case, 16 July 2020.

— CJEU, The Court of Justice invalidates Decision 2016/1250 on the adequacy of the protection provided by the EU-US Data Protection Shield, press release No 91720, 16 July 2020.

— U.S. Department of State, European Court of Justice Invalidates EU-U.S. Privacy Shield, 17 July 2020.

For further information, please contact the TMC team at CMS Albiñana & Suárez de Lezo:

Javier Torre de Silva
Partner | TMC / Data Protection

T +34 91 451 93 21
E javier.torredesilva@cms-asl.com

José Luis Piñar
Of Counsel | TMC / Data Protection

T +34 91 451 40 53
E joseluis.pinar@cms-asl.com

Miguel Recio
Associate | TMC / Data Protection

T +34 91 452 01 90
E miguel.recio@cms-asl.com

This publication does not represent legal advice by its authors. For more information:

cms-asl@cms-asl.com | **cms.law**

C/M/S/ Law-Now™

Law.Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Skopje, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

---

cms.law

CMS Albiñana & Suárez de Lezo

ISO 9001 BUREAU VERITAS Certification