Stanford – Vienna
Transatlantic Technology Law Forum

A joint initiative of
Stanford Law School and the University of Vienna School of Law

TTLF Working Papers

No. 80

EU-US Data Transfers in the Aftermath of the Privacy Shield Invalidation

Nikolaos I. Theodorakis

2021

TTLF Working Papers

Editors: Siegfried Fina, Mark Lemley, and Roland Vogl

About the TTLF Working Papers

TTLF's Working Paper Series presents original research on technology, and business-related law and policy issues of the European Union and the US. The objective of TTLF's Working Paper Series is to share "work in progress". The authors of the papers are solely responsible for the content of their contributions and may use the citation standards of their home country. The TTLF Working Papers can be found at http://ttlf.stanford.edu. Please also visit this website to learn more about TTLF's mission and activities.

If you should have any questions regarding the TTLF's Working Paper Series, please contact Vienna Law Professor Siegfried Fina, Stanford Law Professor Mark Lemley or Stanford LST Executive Director Roland Vogl at the

Stanford-Vienna Transatlantic Technology Law Forum
http://ttlf.stanford.edu

Stanford Law School
Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610

University of Vienna School of Law
Department of Business Law
Schottenbastei 10-16
1010 Vienna, Austria

About the Author

Nikolaos Theodorakis is Of Counsel in the London and Brussels offices of Wilson Sonsini Goodrich & Rosati, where his practice focuses on privacy and cybersecurity. Nikolaos regularly counsels on matters of EU data protection law, GDPR compliance, UK GDPR preparedness, cybersecurity, advertising, and marketing and offers a full cycle of services that includes both non-contentious matters and investigations with supervisory authorities.

Nikolaos represents multinational companies across a wide range of industries, including technology, financial services, healthcare, hospitality, food and beverage, insurance, pharmaceuticals, chemicals, and automotive. He also works with start-ups and established companies in the EMEA region and, in particular, the EU and the UK. Having advised on a broad spectrum of corporate matters, Nikolaos has developed an expert insight into the increasing interplay between data protection, financial services (PSD2), competition law, and international trade law. He is at the forefront of advising on emerging privacy challenges on matters of AI, biotech, fintech, and blockchain.

In addition, Nikolaos is an associate professor of law at the University of Oxford, an assessor at the University of Cambridge, and a fellow at Stanford Law School, focusing on technology and intellectual property issues. Previously, Nikolaos taught and conducted research at the University of Cambridge, Harvard Law School, and Columbia Law School. He also gained professional experience at the U.S. Committee on Capital Markets Regulation, the Kluge Center at the U.S. Library of Congress, and the UK Ministry of Justice.

Nikolaos has received awards from several bodies, including the State Council of the People's Republic of China, the UK Economic and Social Research Council (ESRC), British Academy, and the Greek Parliament. He has been widely published and frequently receives invitations for public engagements, including guest lectures across the world, international symposia, and TEDx conferences.

General Note about the Content

The opinions expressed in this paper are those of the author and not necessarily those of the Transatlantic Technology Law Forum or any of its partner institutions, or the sponsors of this research project.

Suggested Citation

This TTLF Working Paper should be cited as:
Nikolaos I. Theodorakis, EU-US Data Transfers in the Aftermath of the Privacy Shield Invalidation, Stanford-Vienna TTLF Working Paper No. 80, http://ttlf.stanford.edu.

Copyright

Abstract

The Court of Justice of the European Union (CJEU) recently invalidated the EU-U.S. Privacy Shield Framework in its ruling in the Schrems 2 case. The CJEU found that (i) the Privacy Shield does not offer adequate protection to individuals' privacy rights due to potential broad disclosure of personal data to the U.S. intelligence services/public authorities; and (ii) the Ombudsperson created by the Privacy Shield Framework to address complaints by EU citizens lacks the independence and authority to adopt decisions that bind U.S. intelligence services.

The Privacy Shield was relied on by thousands of companies to transfer personal data from the EU to the U.S. under the General Data Protection Regulation (GDPR). Hence, the Privacy Shield's invalidation, in combination with the recent guidance by the European Data Protection Board on supplemental measures to guarantee cross-border transfers, means that companies on both sides of the Atlantic need to carefully reconsider their data transfer strategy. This paper will investigate the background that led to the Privacy Shield invalidation, successor of the also invalidated Safe Harbor, and the options available to transfer data between the EU and the U.S. Finally, the paper will discuss recent trends regarding data transfers, including data localization in Europe.

Table of Contents

1. Introduction

The Court of Justice of the European Union (CJEU) recently invalidated the EU-U.S. Privacy Shield Framework in its ruling in the Schrems 2 case.[1] The CJEU found that (i) the Privacy Shield does not offer adequate protection to individuals' privacy rights due to potential broad disclosure of personal data to the U.S. intelligence services/public authorities; and (ii) the Ombudsperson created by the Privacy Shield Framework to address complaints by EU citizens lacks the independence and authority to adopt decisions that bind U.S. intelligence services.

The Privacy Shield was relied on by thousands of companies to transfer personal data from the EU to the U.S. under the General Data Protection Regulation (GDPR). Hence, the Privacy Shield's invalidation, in combination with the recent guidance by the European Data Protection Board on supplemental measures to guarantee cross-border transfers, means that companies on both sides of the Atlantic need to carefully reconsider their data transfer strategy.

This paper will start by exploring the Safe Harbor, as predecessor of the Privacy Shield, and its invalidation. It will then examine the timeline that led to Privacy Shield's invalidation, followed by the options that are now available to companies to transfer data to third countries. Finally, the paper will discuss recent trends regarding data transfers, including data localization in Europe.

[1] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018], ECLI:EU:C:2020:559

2. The Safe Harbor as the predecessor of the Privacy Shield

Going back to where things first started, in 1980 the OECD issued recommendations for the protection of personal data. These measures were non-binding until 1995, at which point the European Union introduced the EU Data Protection Directive, the predecessor of the General Data Protection Regulation, which paved the path of data protection in the continent and also set the bar of data protection standards around the world.[2]

One of the provisions of the Data Protection Directive was that companies are only permitted to send personal data to so-called "third countries" outside the European Economic Area ("EEA") if they guarantee adequate levels of data protection.[3] With the exception of a few white-listed countries that the European Commission considers to be adequate to the EEA,[4] meaning that they provide an equivalent level of protection and that no further formalities are required when transferring personal data from the EEA to these countries, the majority of the companies that were transferring data abroad would need to rely on other tools. The Binding Corporate Rules are generally time consuming and aimed at large multinational companies (a few more than 100 of those have been approved so far),

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L. 281/31

[3] European Commission, *Adequacy decisions – How the EU determines if a non-EU country has an adequate level of data protection* <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en > accessed 18 October 2021

[4] Countries that are currently considered adequate are: Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland , the United Kingdom under the GDPR and the LED, and Uruguay.

meaning that, in practice, the Standard Contractual Clauses were the most widely used method for transferring personal data from the EEA to third countries.[5]

The Standard Contractual Clauses contain boilerplate language, approved by the European Commission. This means that the parties cannot change or modify the clauses, unless it is to further boost the protection of personal data. The Standard Contractual Clauses, also under their most recent version that was adopted in 2021, are widely used when companies transfer data outside the EU. Since they are an important tool of transferring data across borders, we will further discuss the notion of the Standard Contractual Clauses below.

The Safe Harbor principles were developed soon after the EU Data Protection Directive entered into force to address the complexity around data transfers and to simplify the process of transferring data from the EEA to the US. In essence, the Safe Harbor was a business-driven initiative to facilitate transatlantic data flows and boost economic cooperation on both sides of the pond. The Safe Harbor principles were developed between 1998 and 2000, and the Article 29 Working Party (the predecessor of the European Data Protection Board) is considered a key player that assisted with this process.[6]
The Safe Harbor principles revolved around some commonly accepted principles of protecting the personal data, in an effort to satisfy the requirements otherwise set by the EU Data Protection

[5] European Data Protection Board, *List of Approved Binding Corporate Rules* <https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en> accessed 18 October 2021

[6] Article 29 Data Protection Working Party, *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"*, Adopted on 16th May 2000, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf> accessed 18 October 2021

Directive. Along with these principles, the Safe Harbor committee also published a series of Frequently Asked Questions, describing how the companies participating in the program would be handling personal data.

The seven principles of the Safe Harbor program were:[7]

- **Notice** – Individuals must be informed that their data is being collected and how it will be used. The organization must provide information about how individuals can contact the organization with any inquiries or complaints.
- **Choice** – Individuals must have the option to opt out of the collection and forward transfer of the data to third parties.
- **Onward Transfer** – Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
- **Security** – Reasonable efforts must be made to prevent loss of collected information.
- **Data Integrity** – Data must be relevant and reliable for the purpose it was collected.
- **Access** – Individuals must be able to access information held about them, and correct or delete it, if it is inaccurate.
- **Enforcement** – There must be effective means of enforcing these rules.

[7] Article 29 Working Party on the Protection of Individuals with regard to the Processing of Personal Data, *Opinion 7/99 On the Level of Data Protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents on 15 and 16 November 1999 by the US Department of Commerce*, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/1999/wp27_en.pdf> accessed on 18 October 2021

The European Commission endorsed these Principles and decided, in July 2000, that US companies complying and registering their certification would meet the EU requirements and be included in the so-called "safe harbor scheme". When doing so, companies would be allowed to transfer data from the EU to the US, without any further formality. Notwithstanding the above, the companies transferring data under the safe harbor scheme would need to protect the data in line with the Data Protection Directive requirements.[8]

In terms of regulatory oversight, companies under the authority of the Federal Trade Commission or the Department of Transportation (depending on the company) were eligible to participate in the Safe Harbor scheme, while the US Department of Commerce had the overall oversight. In effect, financial institutions (e.g. banks, investment houses, credit unions, savings & loans institutions) were exempt from the scheme, as well as telecommunication carriers (including internet service providers) and non-profit organizations. All these companies would need to resort to an alternate way to transfer data to the US, and most of them used the SCCs for such purpose.

Pursuant to being included in the program, a company would need to have appropriate employee training in place, and an effective dispute mechanism in place. It would also need to self re-certify every 12 months and represent continuing compliance with the US-EU Safe Harbor Framework

[8] Article 29- Data Protection Working Party, Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, *Opinion 3/2000 On the EU/US dialogue concerning the "Safe harbor" arrangement*, < https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp31_en.pdf> accessed on 18 October 2021

principles as described above. The process of registering with the Safe Harbor was relatively inexpensive (annual fee of $100 for registration) and the penalties for violating the Safe Harbor commitments ranged up to $16000 per day.[9]

Soon after the Safe Harbor program was enacted in 2000, it attracted significant criticism for gaps in the compliance principles compared to what was required under EU Data Protection Law. For instance, in 2002 a European Union review concluded that “a substantial number of organizations that have self-certified adherence to the Safe Harbor do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies" and that "not all dispute resolution mechanisms have indicated publicly their intention to enforce Safe Harbor rules and not all have in place privacy practices applicable to themselves”.[10]

Also, in 2010 local data protection authorities such as the German Data Protection Authorities issued a decision asking companies transferring data from Europe to the US to actively ensure that companies comply with the Safe Harbour principles. The European Commission published a memorandum including 13 recommendations on how to improve the functioning of the Safe Harbor scheme based

[9] Article 29 Data Protection Working Party, *Opinion 4/2000 on the level of protection provided by the “Safe Harbor Principles”*, Adopted on 16th May 2000, <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2000/wp32_en.pdf>, accessed 18 October 2021

[10] Commission of the European Communities, SEC(2002) 196, *The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce*, <https://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/05_2002-196ecstaff_wp_/05_2002-196ecstaff_wp_en.pdf>, accessed 18 October 2021

on a thorough analysis and consultations with companies. In 2014 German Data Protection Authorities further expressed their concern that there is a significant likelihood that the principles in the European Commission's decisions were violated.[11]

Fast forward to 2015, the European Court of Justice responded to a referral from the High Court of Ireland in relation to a complaint from Austrian citizen Maximilian Schrems regarding Facebook's processing of his personal data from its Irish subsidiary to servers in the US. The case related to the NSA/PRISM spy scandal which eventually had major implications for the Safe Harbor Framework and US internet companies operating in Europe.[12] In particular, Schrems complained that "*in the light of the revelations made in 2013 by Edward Snowden concerning the activities of the United States intelligence services (in particular the National Security Agency ('the NSA')), the law and practice of the United States do not offer sufficient protection against surveillance by the public authorities*".[13]

On 23 September 2015 the Advocate General at the Court of Justice of the European Union (CJEU) Yves Bot released his non-binding opinion in the Schrems case C-362/14. There, the AG opined that: (a) mass surveillance systems used by the United States lead to interference with fundamental rights of EU citizens with regard to their privacy; (b) Safe Harbor does not provide adequate protection for EU citizens against this interference and is actually invalid, and (c) the EU Commission decision of

[11] Ernst-Oliver Wilhelm, 'IAPP Resource Center, A brief History of Safe Harbor' <https://iapp.org/resources/article/a-brief-history-of-safe-harbor/> accessed 18 October 2021

[12] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015], ECLI:EU:C:2015:650

[13] European Parliament News, *Mass surveillance: EU citizens' rights still in danger, says Parliament*, 29-10-2015 <https://www.europarl.europa.eu/news/en/press-room/20151022IPR98818/mass-surveillance-eu-citizens-rights-still-in-danger-says-parliament> accessed 18 October 2021

Safe Harbor Adequacy does have the effect of preventing national authorities from investigating a complaint alleging that a third country does not ensure an adequate level of protection and, where appropriate, from suspending the transfer of that data.

On 6 October 2015, the ECJ, in its ruling, held the Safe Harbor Principles to be invalid, since they did not provide sufficient guarantees for US organizations processing EU personal data under the scheme. In particular, the ECJ found that: (a) legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life; (b) that safe harbour scheme enables interference, by U.S. public authorities, with the fundamental rights of persons; (c) that the existence of a European Commission decision finding cannot eliminate or even reduce the powers available to the national supervisory authorities; (d) that supervisory authorities have actually the duty to examine relevant complaints with all due diligence but (e) that the CJEU it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid.[14]

Further, the US federal government agencies could use personal data under US law, but were not required to opt in and, therefore, were "*bound to disregard, without limitation, the protective rules laid down by that scheme where they conflict with national security, public interest and law enforcement requirements*". Overall, the ECJ considered that the US legislation is "*legislation permitting the public authorities to have access on a generalised basis to the content of electronic*

[14] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015], ECLI:EU:C:2015:650

communications must be regarded as compromising the essence of the fundamental right to respect for private life."[15]

Soon after the decision, EU regulators said that if the EU and the United States did not negotiate a new system within three months, businesses could face action from European privacy regulators. The EU and the US quickly started negotiating an updated agreement, which eventually took the form of the Privacy Shield. This led to the announcement of 2 February 2016 that the Privacy Shield "*reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015, which declared the old Safe Harbour framework invalid. The new arrangement will provide stronger obligations on companies in the U.S. to protect the personal data of Europeans and stronger monitoring and enforcement by the U.S. Department of Commerce and Federal Trade Commission, including through increased cooperation with European Data Protection Authorities. The new arrangement includes commitments by the U.S. that possibilities under U.S. law for public authorities to access personal data transferred under the new arrangement will be subject to clear conditions, limitations and oversight, preventing generalised access. Europeans will have the possibility to raise any enquiry or complaint in this context with a dedicated new Ombudsperson*".[16]

[15] David Cole, Federico Fabbrini, Stephen Schulhofer, *Surveillance, Privacy and Trans-Atlantic Relations*, Bloomsbury Publishing 2017, p. 55

[16] European Commission Press Release, *EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield*, 2 February 2016 <https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216> accessed 18 October 2021

3. The Privacy Shield and Its Invalidation

In February 2016, the EU Commission announced an agreement with the US on the EU-US Privacy Shield, which is built around the elements of: (i) strong obligations on companies handling EU personal data and robust enforcement, (ii) clear safeguards and transparency obligations on US government access, (iii) and effective protection of EU citizens' rights with several redress possibilities (including an ombudsman). However, immediately after the creation of the Privacy Shield several civil rights organizations declared that they do not believe that the Privacy Shield between the US and the EU meets the standards set by the Court of Justice of the European Union (CJEU).[17] In particular, the criticism revolved around the idea that reforms do not ensure protection for fundamental rights on both sides of the Atlantic, undermine trust in the digital economy, and perpetuate human rights violations.

Under the Privacy Shield, U.S. companies guaranteed that they would meet seven principles when handling EU-originating personal data, which included:[18]

- **Notice:** Individuals must be notified about the collection and use of their personal information.
- **Choice:** Organizations must give individuals the opportunity to opt out of the disclosure of their personal data to third parties.

[17] European 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-US Privacy Shield (notified under document C(2016) 4176) [2016] OJ L207/1

[18] European 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-US Privacy Shield (notified under document C(2016) 4176) [2016] OJ L207/1

- **Accountability for Onward Transfers:** Organizations are accountable for applying the notice and choice principles in order to disclose personal data to third parties.
- **Access:** Individuals must be able to access their personal data being stored by an organization.
- **Security:** Organizations must protect personal data from loss, misuse, unauthorized access, and disclosure.
- **Data Integrity**: Organizations must ensure data is reliable and relevant for the purpose it is being used.
- **Recourse, Enforcement, and Liability:** Individuals have the right to affordable recourse mechanisms if they believe their personal data has been misused.

The Privacy Shield became a highly popular mechanism and approximately 5,500 US companies subscribed to it.

Even though the US and the European Commission made improvements to the Safe Harbor program in an effort to address the ECJ's concerns in a targeted way, a new round of legal challenges was just around the corner.[19] Max Schrems filed a complaint with the Irish Data Protection Commissioner, challenging Facebook Ireland's use of the SCCs as a transfer mechanism. The Irish High Court referred the matter to the ECJ, including a wide-ranging list of questions that challenged the validity of the SCCs. The list was comprehensive and included a breadth of topics covering data transfers and relevant safeguards. In particular, the questions were:[20]

[19] The CJEU judgment in the Schrems II case, European Parliament <https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf> accessed 18 October 2021

[20] Thomas Shaw, 'The CJEU's 11 key questions in Schrems II' (2018), IAPP Privacy Advisor <https://iapp.org/news/a/the-11-key-considerations-in-schrems-ii-in-laymans-terms/> accessed 18 October 2021

1. When personal data is transferred from the EEA under SCCs, knowing it may be further processed by the security services of the receiving country, do the rights in the Charter apply, despite derogations allowed in the Treaty of the EU and the Data Protection Directive limiting data protection rights for reasons of national security, defense, public safety, and national economic interests?
2. When analyzing transfers of personal data outside the EEA, should violations be measured against the rights in the Charter, the TEU, the Treaty on the Function of the EU, the DPD, the Convention on Human Rights, or some other EU or member state law?
3. When personal data is transferred outside the EEA under SCCs, is the adequacy of the measures in the recipient country determined only on that country's laws and compliance practices or must it also include "administrative, regulatory and compliance practices and policy safeguards, procedures, protocols, oversight mechanisms, and non-judicial remedies?
4. If personal data is transferred from the EU to the U.S. under the SCCs, does it violate Article 7 (privacy) and Article 8 (data protection) rights under the Charter, based on the findings of the court?
5. If personal data is transferred from the EU to the U.S. under the SCCs, does it violate the Article 47 right under the Charter to an effective judicial remedy, based on the findings of the court, and if not, are the U.S. law restrictions on data protection rights for national security proportionate and necessary?
6. What level of protection is required for personal data transferred outside the EEA under SCCs, in respect to both the Charter and the DPD?

7. Do mandates by recipient country governments to make personal data available for inspection by its security services make it impossible for there to be adequate safeguards under the DPD for SCCs?
8. When a DPA finds that the surveillances laws in countries receiving EEA personal data conflict with the SCCs, is the DPA: required to suspend data flows, suspend data flows only in exceptional cases, or can the DPA use its discretion to not suspend the data flows?
9. Is the Privacy Shield decision binding on member state courts and DPAs in that it means that the U.S. offers an adequate level of protection? But if it does not, what role does the Privacy Shield adequacy finding have on the adequacy evaluation for SCCs?
10. Does the role of the Privacy Shield ombudsman in the context of the U.S. privacy regime ensure the Article 47 right to a judicial remedy for personal data transferred from the EEA?
11. Does the EC's SCC decision itself violate the rights to privacy, data protection, and an effective judicial remedy under the Charter?

On December 19, 2019 the Advocate General opined that the SCCs are valid since they are designed in a way to provide continuous and adequate protection to the personal data no matter where the data is based.[21] The AG offered a way out to the ECJ regarding the Privacy Shield since he opined that the ECJ could make a defensible argument that it does not need to examine the Privacy Shield's validity

[21] Court of Justice of the European Union, Press Release No 165/19, "*According to Advocate General Saugmandsgaard Øe, Commission Decision 2010/87/EU on standard contractual clauses for the transfer of personal data to processors established in third countries is valid.*", <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-12/cp190165en.pdf> accessed 18 October 2021

in this ruling. The AG also extended a word of caution in that, if the ECJ were to ultimately examine this, there are concerns about the conformity of the Privacy Shield with the GDPR.

Notwithstanding the above, the European Court of Justice (ECJ) declared the EU-US Privacy Shield framework invalid on 16 July 2020. In its ruling, the ECJ upheld the EU Standard Contractual Clauses (SCCs) but confirmed that the companies must verify prior to any transfer using SCC that the parties can effectively provide the level of protection required by EU law.[22]

The ECJ ultimately invalidated the Privacy Shield on two grounds: (i) it does not offer adequate protection to individuals' data protection rights in light of the broad disclosure of personal data to the US intelligence services; and (ii) the Ombudsperson included in the Privacy Shield framework was not practically effective and did not address complaints received by EU citizens, also contributing to an overall lack of independence and authority to adopt decisions that are binding on US intelligence services.[23]

In particular, the ECJ ruled that U.S. domestic law does not offer a standard of legal protection that is "essentially equivalent" to the standard of protection under EU law. The ECJ found that national intelligence programs authorized by Section 702 of the Foreign Intelligence Surveillance Act (FISA)

[22] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018], ECLI:EU:C:2020:559, paras 44 et seq.

[23] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018], ECLI:EU:C:2020:559, paras 54 et seq.

and Executive Order 12333 do not grant EU individuals actionable rights before the courts against U.S. authorities, rendering the data protection rights insufficient.[24]

The ECJ noted that the Charter of Fundamental Rights of the European Union (Charter) protects individuals' private communications and personal data. Disclosing data to a third party—including public authorities—interferes with these rights, and is permitted only if strictly necessary. However, the ECJ indicated that surveillance programs like Presidential Policy Directive-28 regarding signals intelligence activities may process a disproportionate amount of data and allow access to data in transit to the U.S. without any judicial review. The ECJ reasoned that the surveillance programs are not limited in scope and do not provide guarantees for potentially targeted non-U.S. individuals. As such, individuals do not have an effective judicial remedy to exercise their privacy rights.[25]

The ECJ further found that the Privacy Shield's Ombudsperson mechanism cannot remedy the deficiency described above because it lacks the power a tribunal traditionally has. In particular, the Ombudsperson lacks the authority to bind U.S. intelligence services. As a result, EU citizens have no redress mechanism for certain surveillance activities.

The ECJ also opined that the Ombudsperson lacks independence because he is appointed by the Secretary of State and is an integral part of the U.S. State Department. The Ombudsperson reports

[24] Section 702 overview <https://www.dni.gov/files/icotr/Section702-Basics-Infographic.pdf> accessed 18 October 2021

[25] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018], ECLI:EU:C:2020:559, paras 56 et seq.

directly to the Secretary of State, and there are no guarantees to protect against the revocation or dismissal of the Ombudsperson, which undermines his independence.

Based on the above, the ECJ invalidated the Privacy Shield. Notwithstanding the substantial business disruption this ruling creates, the Court noted that it does not believe the invalidation creates a legal vacuum since companies can still rely on other transfer mechanisms, including the GDPR's list of derogations (e.g., consent).

4. Companies' Options Pursuant to the Privacy Shield Invalidation

Pursuant to the invalidation of the Privacy Shield, companies are left with fewer options when they want to transfer personal data outside the European Economic Area, as we will discuss below. Notwithstanding these options, transatlantic trade was affected by this development since several companies relied on the Privacy Shield to transfer data across the pond.

In particular, Chapter V of the GDPR permits data transfers to third countries under certain conditions:[26]

- If the country is included in the European Commission's adequacy list (currently including Andorra, Argentina, Canada (commercial organizations), Faroe Islands, Guernsey, Israel, Isle of Man, Japan, Jersey, New Zealand, Switzerland , the United Kingdom under the GDPR and the LED, and Uruguay).

[26] 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), OJ L 119, 4.5.2016, p. 1–88

- The company adopts Standard Contractual Clauses (SCCs), which are boilerplate contracts approved by the European Commission and furnishing a level of protection that is commensurate to that of the GDPR.
- If a company applies for Binding Corporate Rules, which are considered the "gold standard" for data protection standards.
- If a company complies with Codes of conduct approved by a supervisory authority (currently this has not been the case yet).
- If a company relies on one of the GDPR derogations. The GDPR includes certain derogations that permit, as an exception, data transfers to third countries. The most used GDPR derogations include consent, and contract performance (i.e. that the data transfer is required to perform the contract that the individual has requested from the company).

4.1. Standard Contractual Clauses

The Standard Contractual Clauses are arguably the most popular way to transfer personal data from the EU to the US pursuant to the Privacy Shield invalidation. In its referral, the Irish High Court had posed several questions regarding the validity of the SCCs, including whether SCCs are capable of ensuring adequate protection if they do not bind the public authorities of the foreign country.

The European Court of Justice did not invalidate the SCCs, yet it introduced certain criteria that companies needed to take into account before using the SCCs. This, partly, has to do with the fact that the SCCs were initially enacted in 2001 to correspond with the then reality of the EU Data Protection Directive. As such, it is rather expected that they did not fully satisfy the legal and practical reality 20 years later, particularly in light of the GDPR. As a result, the SCCs received a significant facelift, more on which we will discuss in the following chapters.

By upholding the SCCs, the court also tightened the requirements that accompany them, without however giving a grace period. Almost immediately, enforcement activities in Ireland questioned the validity of the SCCs whereas in other countries like Germany regulators left the door open to further challenges.

The ECJ explained that the SCCs are a form of appropriate safeguards, which should be distinguished from adequacy decisions. An adequacy decision is based on an assessment of the level of protection of personal data afforded by a particular legal system as a whole, which renders all organizations within that legal system eligible to receive personal data from the EU. Unlike adequacy decisions, the GDPR's provisions on appropriate safeguards specifically allow the EU Commission to adopt standard data protection clauses to govern transfers between data exporters and data importers, irrespective of the legal system of the data importers. As a result, the validity of the SCCs does not depend on, and the EU Commission did not need to assess, the adequacy of the countries to which data could be transferred using SCCs.[27]

Whether SCCs constitute appropriate safeguards, however, depends on whether the SCCs incorporate effective mechanisms to ensure compliance with the level of protection required by EU law. The European Court of Justice concluded that the SCCs do incorporate effective mechanisms, in part because of the obligation on importers to inform exporters when they cannot comply with the SCCs, and the obligation on exporters to subsequently suspend the transfer.

[27] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018], ECLI:EU:C:2020:559, paras 74 et seq.

Organizations and regulators must assess compliance with Standard Contractual Clauses

Because, among other things, the SCCs do not bind public authorities, the ECJ determined that it may be necessary to supplement the guarantees provided by the SCCs. The ECJ explained that it is up to the organizations to verify on a case-by-case basis and prior to any transfer whether the SCCs can afford the requisite level of protection required by the GDPR and, where necessary, to implement further safeguards.[28]

For ongoing transfers, exporting organizations must suspend or stop data transfers if they can no longer provide the requisite protection to EU citizen data. Consistent with the provisions of the current SCCs, the ECJ explains that importing organizations must inform exporters if they are no longer able to comply with the SCCs, in which case the exporter is required to suspend the transfer.

Furthermore, if a regulator determines that the SCCs cannot be complied with in a particular country of import, and the required level of protection cannot be provided by other means, the regulator must suspend or prohibit the transfer.

4.2. Binding Corporate Rules

Binding Corporate Rules (BCRs) are a set of rules that describe how a company internally processes personal data within its different entities. It has been considered the gold standard of privacy, however it is also a costly and lengthy process, and therefore may not be a practical option for certain

[28] Case C-311/18 *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* [2018], ECLI:EU:C:2020:559, paras 87 et seq

companies. In fact, only a handful of companies globally have received BCR approval, primarily large multinational companies. This means that such intense exercise is not fit for purpose for small and medium-sized companies.

4.3. Derogations

The GDPR derogations are an increasingly popular means to transfer personal data outside the EU, particularly in cases where individuals are transferring personal data. Derogations are only intended for specific purposes, e.g. contract performance.[29] Also, where a company is using consent as an appropriate derogation, that consent must be unambiguous, unbundled from any other service offering, and after the individual has been clearly made aware of the consequences of his data exiting the EU.

4.4. Privacy Shield

The Privacy Shield was enacted only after a few months of the Safe Harbor's invalidation. Yet, it appears that the successor of the Privacy Shield, if any, will not be as a straightforward process. The timeline of the replacement is currently unknown, and as per below the countries involved continue to reiterate the need to come up with a meaningful process.

[29] The relevant derogations according to Art. 49 of the GDPR are: (a) the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request; (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person; (d) the transfer is necessary for important reasons of public interest; (e) the transfer is necessary for the establishment, exercise or defence of legal claims; (f) the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent; (g) the transfer is made from a register which according to Union or Member State law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.

The US Department of Commerce has also expressed that it will continue to administer the Privacy Shield program, including self-certifications and recertifications. It further stated that the ECJ's decision does not relieve companies from their Privacy Shield obligations, meaning that companies cannot simply stop observing the Privacy Shield obligations, and that they need to continue to abide by them until they revoke or do not renew their certification. This is irrespective of whether Companies rely on the Privacy Shield as a lawful way to transfer personal data from the EU to the US (since they can no longer rely on this pursuant to the Privacy Shield invalidation).

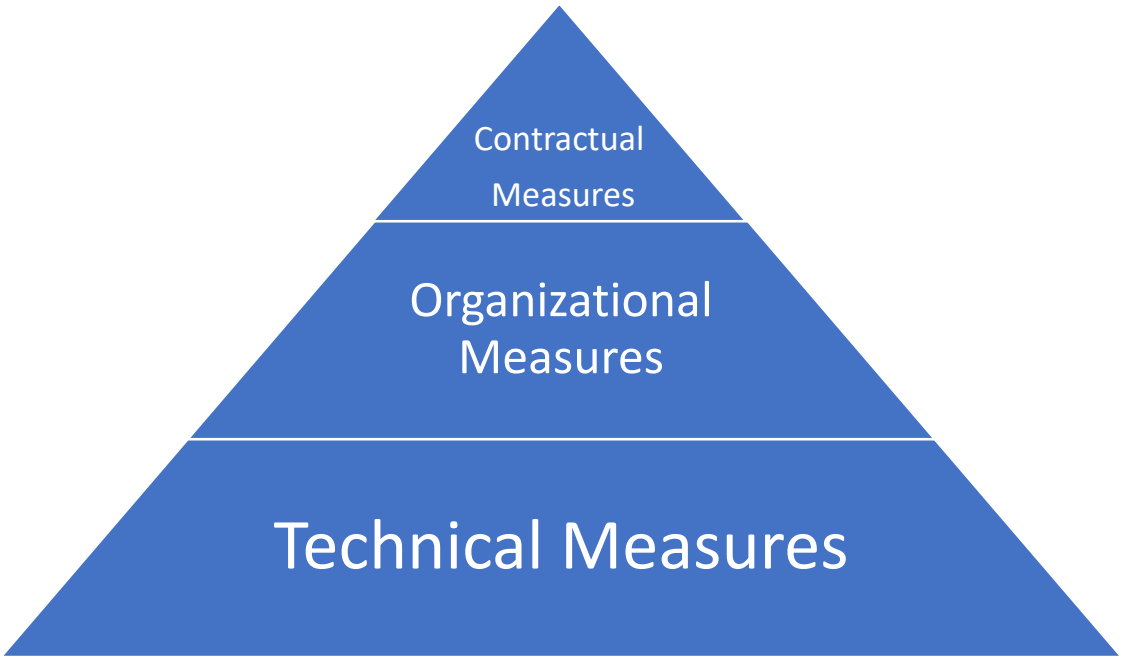
5. Implications for Companies and Future Trends

The implications for US companies were overall significant since the invalidation of the Privacy Shield reinforced the reliance on Standard Contractual Clauses for transatlantic data transfers, but also led to an increased trend of data localization. As we will discuss below, the new SCCs are overall a very popular way to transfer data from the EEA to the US, however such transfers still require a case-by-case assessment of the data transfer through a Data Transfer Impact Assessment (DTIA).

5.1. The new Standard Contractual Clauses

The European Commission published the new Standard Contractual Clauses on 4 June 2021, and they entered into force on 27 September 2021. This means that the new Standard Contractual Clauses need to be used with any new contract where data transfers outside the EU are envisaged. For existing contracts, the transition period to the new SCCs ends on 27 December 2022, unless the parties update or amend the contract in the meantime, in which case they are required to use the new SCCs irrespectively.

Even though the European Court of Justice did not annul the Standard Contractual Clauses in 2020, it expressed certain concerns with respect to their effectiveness. These concerns were further discussed by the European Data Protection Board, which issued guidelines on how to effectively protect the data when relying on the SCCs. In particular, companies can use so-called supplemental measures. These measures can be technical (e.g. encryption, pseudonymization etc.), organizational (e.g. internal process to handle and scrutinize government requests) and contractual (e.g. contractual requirements with vendors to adequately protect the data in question). The EDPB recommendations overall represent a consensus among supervisory authorities in interpreting the Schrems 2 decision.

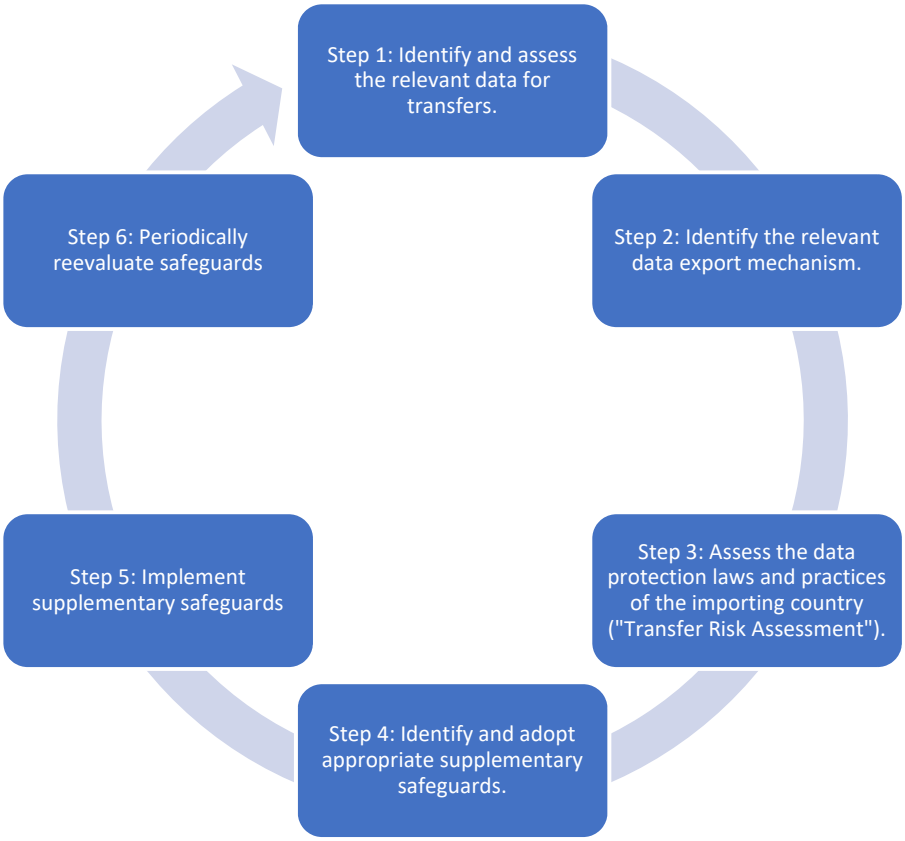


Pyramid of supplemental measures as described by the European Data Protection Board

The EDPB guidelines also include certain steps that companies need to follow when they assess whether they can transfer personal data to third countries. In practice, this means that companies can no longer solely rely on the SCCs when transferring data to third countries, but they also need to assess

the potential risk, and whether they can objectively transfer the data without impinging on their protection.

The six steps of the EDPB data transfer methodology are the following:



In the first step, companies need to know their transfers. This is typically done through data maps, where companies include their transfers and onward transfers of data to third countries. This can be a challenging exercise, intense in resources. It is primarily a data exporter obligation (i.e. the company that transfers data outside the EEA), however data importers will likely receive questions on onward transfers from EU business partners.

In the second step, companies need to identify the relevant data export mechanism on which they rely to transfer data abroad. No further action is required if a country is white-listed (i.e. considered

adequate) or if companies rely on derogations to process data (e.g. consent or contract performance). However, if companies rely on one of the GDPR Art. 46 safeguards to transfer the data (BCRs, Standard Contractual Clauses, National Standard Contractual Clauses, Codes of Conduct, Certification, Ad ho Contract), they need to take further action and complete the remaining steps of this exercise.

In the third step, companies need to conduct a transfer risk assessment (TRA), in which they assess the facts of the transfer (e.g. nature of data and destination country), the applicable laws relevant to the transfer, whether and how these laws impact the effectiveness of the transfer mechanism, as well as the relevant outcome and the actions advised or taken based on the above.

In the fourth step, companies assess the practical considerations, and whether the supplemental measures adopted can alleviate the data transfer concerns. A relevant question is, therefore, when are supplementary measures considered sufficient, and how can companies continuously scrutinize said measures to ensure they remain up to date.

In the fifth step, companies are encouraged to implement the supplementary safeguards that they have identified as relevant to alleviate the data protection concerns. Finally, in the sixth step, companies are reminded to periodically re-evaluate the safeguards and monitor developments in third countries on an ongoing basis. Accountability is a continuing obligations and companies need to have mechanisms in place to suspend/end transfers where a data importer has breached/cannot comply with commitments, or where supplementary measures are no longer effective in a third country.

The new SCCs take into account the ECJ's concerns, and incorporate some of the European Data Protection Boards' recommendations. They are therefore more protective compared to the old SCCs, and they revolve around the requirements of the GDPR rather than the EU Data Protection Directive. They also offer greater flexibility since they allow data transfers also from processors based in the EU (processor-processor and processor-controller), whereas under the old SCCs data transfers could only originate from controllers based in the EU (controller-controller and controller-processor).

Even though the new SCCs offer greater flexibility regarding data transfers and they are tailored to the GDPR's requirements, they do not relief companies from their obligation to conduct Data Transfer Impact Assessments (DTIAs) to assess whether a transfer to a third country is permitted, what are the risks associated with said transfer, the measures taken to mitigate such risk, and whether these measures are adequate. DTIAs are still a work in progress since several companies are trying to find an efficient way to make these work.

Despite the creation of the new SCCs, the UK is still endorsing the old SCCs since they were enacted prior to the Brexit, but has not adopted the new SCCs. As a result, companies that have operations in the UK and the EU, sending data to the US, need to use the new SCCs for the EU data transfers and the old SCCs for the UK data transfers. This creates a certain fragmentation, but also an uneven playing field for data protection since the new SCCs generally afford greater protection to the data compared to the old SCCs. This paradox is further puzzling since the UK is considered an adequate country, meaning that the European Commission allows data transfers from the EU to the UK without any formality. This means that, notwithstanding the new SCCs, an EU-based company can transfer data to

the UK without any formality, and then onward transfer the data from the UK to the US based on the old SCCs, therefore entirely bypassing the new SCCs.

The UK is, however, in the process of drafting its own set of data transfer tools, which will be formalized in the course of the next months. In particular, the Information Commissioner's Office (ICO) published a draft international data transfer agreement (IDTA) and guidance to replace the SCCs. The ICO recently launched a public consultation, which closed on 11 October 2021. It remains to be seen how the UK's finalized IDTA will interact with the new EU SCCs.[30]

5.2. Towards a new Privacy Shield?

Soon after the Schrems II judgment, the European Commission and the US Department of Commerce initiated discussions on evaluating the potential for an enhanced EU-US Privacy Shield framework to comply with the judgement of the European Court of Justice in the Schrems II case. Even though the Privacy Shield was finalized only a few months after the Safe Harbor invalidation, it was clear from the beginning that a "new" Privacy Shield would not be a straightforward task. In fact, academics and privacy experts throughout Europe have been quite reserved, if not pessimistic, as to whether a new Privacy Shield was an attainable goal, and in any event an imminent one.

The US has repeatedly reiterated its commitment to work with the EU and ensure continuity in transatlantic data flows. The US Department of Commerce took into account the European Data

[30] Information Commissioner's Office, *ICO consults on how organisations can continue to protect people's personal data when it's transferred outside of the UK*, <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk/> accessed 18 October 2021

Protection Board's suggestions, and posited that it was prepared to initiate negotiations on the successor agreement to the EU-US Privacy Shield.

In terms of progress so far, reports have been mixed ranging from active optimism to active pessimism. In a joint statement, the EU Commissioner for Justice, Didier Reynders, and U.S. Secretary of Commerce, Gina Raimondo**,** made the following statement regarding the negotiations on transatlantic data privacy flows:[31]

"The U.S. Government and the European Commission have decided to intensify negotiations on an enhanced EU-U.S. Privacy Shield framework to comply with the July 16, 2020 judgment of the Court of Justice of the European Union in the Schrems II case.

These negotiations underscore our shared commitment to privacy, data protection and the rule of law and our mutual recognition of the importance of transatlantic data flows to our respective citizens, economies, and societies.

Our partnership on facilitating trusted data flows will support economic recovery after the global pandemic, to the benefit of citizens and businesses on both sides of the Atlantic."

The new SCCs and the EDPB recommendations will not necessarily influence talks regarding a Privacy Shield replacement, but rather highlight the need for a government solution to address this. The primary focus would be both for the EU and the US to craft a strong data transfer agreement that avoids the downsides of the Privacy Shield (and Safe Harbor before it).

[31] European Commission, *Intensifying Negotiations on transatlantic Data Privacy Flows: A Joint Press Statement by European Commissioner for Justice Didier Reynders and U.S. Secretary of Commerce Gina Raimondo (*25 March 2021), <https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_21_1443> accessed 18 October 2021

In terms of when will the new deal on transatlantic data flows materialize, this truly depends based on several variables. Since the ECJ annulled the so-called Privacy Shield agreement, negotiators on both sides of the Atlantic have been working on a replacement deal designed to shuttle Europeans' data to the US with adequate guarantees.

Recently, the US has claimed that it has introduced enhanced solutions to overcome pending issues where an agreement is not currently available. It remains to be seen whether the recently launched EU-US Trade and Technology Council will act as a catalyst and expedite this process, or whether some ongoing thorny issues will continue to delay the agreement. The EU has generally been less vocal in when a deal is due, and has overall maintained that an agreement before the end of 2021 is not the default scenario. In particular, a key sticking point is how the US can effectively limit how American national security agencies access European data, and provide to EU citizens a meaningful way to challenge such access in US courts.

The US has been trying to streamline data flow discussions, however the free flow of data with privacy protection standards is essential for companies, particularly since they want to remain competitive. A key aim is for the parties to bridge the gaps between their data protection systems, and the commonalities that are enshrined accordingly.

5.3. What about data localization?

Based on the sections above, a reasonable question that companies both in the US and the EU have been asking is whether data localization is the way forward. Companies and regulators are therefore invited to address the question whether the new rules will have the effect of hard data localization,

which would as a result limit several routine data flows from the EU. For instance, concerns regarding hard data localization include technical obstacles to providing online services, fewer options when providing such services, and potential cybersecurity risks as a result of extensive data localization.

As such, even though data localization may sound as an easy fix, it is in fact time, energy and money consuming, while it potentially exposes data to more risks than regular cloud storage. Certain countries have recently introduced laws that include data localization provisions. Even though such provisions hamper technological innovation and growth, some countries seem to favor them since they can exert complete and holistic control over the data processed within their jurisdiction.

The debate regarding data localization has been increasing and vivid, however it has not yet led to the determination that this is the mainstream result, and that countries should be following this. Over the past years, the effects and the downsides of data localization have become apparent, and academic research in the field has also attempted to flesh those out in a concrete way.

Overall, what is potentially more protective to the data, than simply going all-in to data localization is the companies' ongoing efforts to catalogue their processing activities, and internally document how, why, where and when data is being processed. For instance, companies can embark into data mapping efforts to fully understand their data in different layers and catalogue said data across systems and processes. They can also follow the general GDPR principles of data minimization (only collect the data that is needed, only for the period of time that it is needed), purpose limitation (only collect the data for specific purposes explained to the data subject at the time of the collection), transparency

(through a privacy notice that thoroughly explain what happens to individuals' data) and disclosures (through an explanation of exactly where data goes, and to which countries).

The field of data transfers has been fast moving over the past years, if not months, and it is almost impossible to predict what the next years hold for EU/UK-US data transfers. When all is said and done, the introduction of the new SCCs provides a valuable lifeline for transatlantic data transfers. This is irrespective of whether a new Privacy Shield will be introduced, which is likely but not certain at the moment, and the increasing trend of data localization which essentially contradicts the concepts of free trade and increased data flows, values on which the GDPR itself was drafted.