The EU–US data privacy framework and the impact on companies in the EEA and USA compared to other international data transfer mechanisms

Lothar Determann

Baker McKenzie LLP, USA

Lothar Determann works at Baker McKenzie in San Francisco and Palo Alto. He has been counselling companies since 1998 on data privacy law compliance and taking products and business models international. Admitted to practice in California and Germany, he has been recognised as one of the top ten copyright attorneys and top 25 intellectual property attorneys in California by the *San Francisco & Los Angeles Daily Journal* and as a leading lawyer by Chambers, Legal 500, IAM and others. For more information see www.bakermckenzie.com. Prof Dr Determann has been a member of the Association of German Public Law Professors since 1999 and teaches data privacy law, computer law and internet law at Freie Universität Berlin (since 1994), University of California, Berkeley School of Law (since 2004), Hastings College of the Law (since 2010), Stanford Law School (2011) and University of San Francisco School of Law (2000–2005). He has authored more than 150 articles and treatise contributions as well as five books, including 'Determann's Field Guide to Data Privacy Law' (5th Edition, 2022, also available in Arabic, Chinese, French, German, Hungarian, Italian, Japanese, Korean, Portuguese, Russian, Spanish and Turkish) and 'California Privacy Law — Practical Guide and Commentary on U.S. Federal and California Law' (5th Ed. 2023). His 'Field Guide to Artificial Intelligence Law' is scheduled to be published in January 2024. Recent papers include 'Healthy Data Protection', 'Electronic Form over Substance' and 'No One Owns Data'.

Baker McKenzie LLP, 600 Hansen Way, Palo Alto, CA 94304, California, USA
Tel: +1 650 8565533, E-mail: ldetermann@bakermckenzie.com

Michaela Nebel

Baker McKenzie, Germany

Michaela Nebel is an attorney at Baker McKenzie's Frankfurt office and co-head of the German Information Technology Group. She advises companies on all aspects of information technology law and digital law, with a strong focus on data protection law and data dispute matters. She is the author of numerous articles on information technology law and data protection law and the co-author of an English language commentary on the EU General Data Protection Regulation. Michaela holds a PhD in law and certifications as a Certified Information Privacy Professional/Europe (CIPP/E) and a Certified Information Privacy Professional/US (CIPP/US).

Baker McKenzie Rechtsanwaltsgesellschaft mbH von Rechtsanwälten und Steuerberatern, Junghofstraße 9, 60315 Frankfurt/Main, Germany
Tel: +49 69 2 99 08 502; E-mail: michaela.nebel@bakermckenzie.com

Michael Schmidl

Co-head of the German Information Technology Group, Baker McKenzie, Germany

Prof Dr Michael Schmidl is co-head of the German Information Technology Group and is based in Baker McKenzie's Munich office. He is an honorary professor at the University of Augsburg and specialist lawyer for information technology law (Fachanwalt für IT-Recht). He advises in all areas of contentious and non-contentious information technology law, including Internet, computer/software, data privacy and

media law. Michael also has a general commercial law background and has profound experience in the drafting and negotiation of outsourcing contracts and in carrying out compliance projects.

Baker McKenzie, Theatinerstrasse 23, 80333 Munich, Germany
Tel: +49 89 5 52 38 211, E-mail: Michael.Schmidl@bakermckenzie.com

Abstract Third time's a charm? Companies in the European Economic Area, Switzerland and the UK (EEA+) are considering the pros and cons of the third attempt of the EU Commission and US government to establish interoperability between their data protection and privacy law systems, after the demise of the US Safe Harbor Program and the EU–US Privacy Shield. Should US companies register? Are the efforts worth the potential benefits, given that the new programme has already been challenged and may be invalidated like previous programmes for reasons that businesses cannot control? Should companies that were already enrolled in the previous programmes accept automatic enrolment or leave the programme? Can and should companies in the EEA+ rely on EU–US Data Privacy Framework (DPF) registration for international transfers? Or insist on registration in addition to standard contractual clauses (EU SCC 2021) or other compliance mechanisms? Are data transfer impact assessments (DTIAs) still required for transfers to the US? Should they be updated? This paper seeks to help companies find answers to these questions and (I) outlines the background and context of the Adequacy Decision, (II) explains how US companies can join the DPF, (III) discusses the impact of the Adequacy Decision, (IV) summarises requirements for other compliance mechanisms for international data transfers under the GDPR, (V) compares the DPF to other transfer compliance mechanisms and (VI) provides practical considerations and a summary.

KEYWORDS: EU–US Data Privacy Framework, EU–US Privacy Shield, US Safe Harbor Program, GDPR, data protection law, international data transfers, data transfer impact assessments, three hurdles

INTRODUCTION

On 10th July, 2023, the European Commission adopted a decision (Adequacy Decision),[1] according to which the US ensures an adequate level of protection for personal data transferred from the EU to organisations in the US that are included in the 'Data Privacy Framework List'[2] for the purpose of Article 45 of the EU General Data Protection Regulation (GDPR). This article (I) outlines the background and context of the Adequacy Decision, (II) explains how US companies can join the EU–US Data Privacy Framework (DPF), (III) discusses the impact of the Adequacy Decision, (IV) summarises requirements for other compliance mechanisms for international data transfers under the GDPR, (V) compares the DPF to other transfer compliance mechanisms and (VI) provides practical considerations and a summary.

BACKGROUND AND CONTEXT

Companies that are subject to the GDPR are prohibited from transferring personal data to companies outside of the European Economic Area (EEA), unless they overcome three hurdles, which are that companies must (1) comply with the GDPR and supplementary data protection laws, which includes finding a lawful basis to collect and process personal data, issuing a privacy notice, and complying with numerous other requirements; (2) overcome a general prohibition to transfer personal

data to other controllers under Article 6 and Article 9 of the GDPR and (3) overcome a general prohibition of transferring personal data to countries outside the EEA under Article 44 *et seq*. of the GDPR. The DPF and this paper focus only on this third hurdle, but companies have to be mindful about also addressing the first two hurdles in order to comply with the GDPR.

With regard to the said third hurdle, the prohibition of international data transfers, the GDPR offers a number of different compliance mechanisms to legitimise transfers, including (a) an adequacy decision under Article 45 of the GDPR with respect to particular countries, (b) appropriate safeguards under Article 46 of the GDPR, which includes binding corporate rules (BCRs) that affiliated groups of companies can adopt and submit for approval by data protection authorities, and standard contractual clauses (SCCs) that companies can sign with affiliated and unaffiliated companies, and (c) derogations under Article 49 of the GDPR, including explicit consent from data subjects and the need to draw up a contract between the data subject and the controller.

The European Commission has issued adequacy decisions for Andorra,[3] Argentina,[4] Canada,[5] Faroe Islands,[6] Guernsey,[7] Israel,[8] Isle of Man,[9] Japan,[10] Jersey,[11] New Zealand,[12] the Republic of Korea,[13] Switzerland,[14] the UK[15] and Uruguay.[16] Concerning the US, the European Commission had previously adopted limited adequacy decisions covering only companies that voluntarily joined EU law-specific compliance programmes. In 2000 the European Commission adopted the 'Safe Harbor decision',[17] pursuant to which the US provided an adequate level of data protection with respect to US companies that voluntarily joined the US Safe Harbor Program and promised to comply with 'Safe Harbor principles' that reflected requirements of EU data protection laws. In its Schrems I decision of 6th October, 2015, the Court of Justice of the European Union (CJEU) declared the European Commission decision regarding Safe Harbor invalid, mainly due to concerns regarding surveillance activities of the US government for national security purposes.[18] In 2016 the European Commission adopted the 'Privacy Shield decision'[19] concerning US companies that joined the EU-US Privacy Shield programme, which succeeded the US Safe Harbor Program. In its Schrems II decision of 16th July, 2020, the CJEU declared the European Commission's decision concerning the Privacy Shield invalid,[20] again mainly because of concerns regarding US government surveillance for national security purposes.

In the Schrems II decision, the CJEU acknowledged that its concerns regarding US government surveillance do not only apply in respect of personal data transferred to US companies that participate in the EU–US Privacy Shield, but also to data transfers under the EU SCCs.[21] Although the CJEU decided that the European Commission's decision on the SCCs remains valid, the CJEU requires controllers and recipients to assess whether the third country offers guarantees ensuring an adequate level of protection that is 'essentially equivalent' to that ensured within the EU. If this cannot be ensured, companies must adopt supplementary measures in order to ensure compliance with that level of protection. The assessment of whether the third country offers guarantees ensuring an adequate level of protection that is essentially equivalent to that ensured within the EU (known as a data transfer impact assessment) and the implementation of supplementary measures is quite challenging for companies, particularly in light of the strict interpretation of the data protection authorities.[22] Even small and medium-sized companies in the EEA work with dozens or hundreds of technology and service providers, which in turn use other providers in many different jurisdictions, resulting

in myriad international data transfers to be assessed with elaborate documentation.

On 25th March, 2022 the European Commission and the US announced an 'agreement in principle' on a new Trans-Atlantic Data Privacy Framework, according to which the United States must specifically implement safeguards to limit data access by US intelligence authorities and establish a new redress mechanism including a 'Data Protection Review Court'.[23] The US then adopted Executive Order 14086 on enhancing safeguards for US intelligence activities on 7th October, 2022.[24] On 13th December, 2022, the European Commission published a draft adequacy decision, including an annex with the EU-US DPF. The European Data Protection Board adopted an opinion on the European Commission draft implementing decision on the adequate protection of personal data under the EU–US DPF in February 2023.[25] On 3rd July, 2023 the US issued a statement saying that the US has fulfilled its commitments in terms of implementing the EU–US DPF.[26] On 10th July, 2023 the European Commission adopted its Adequacy Decision concerning the EU–US DPF.

HOW CAN US COMPANIES JOIN THE DPF?

The US Department of Commerce operates the DPF as it also operated the US Safe Harbor Program and the EU–US Privacy Shield programme. Even after the Schrems II decision, the US continued operating the EU–US Privacy Shield programme and many US companies continued annual self-certifications, hoping that a successor programme would eventually emerge. When the EU–US DPF went live, it automatically enrolled US companies that participated in the EU–US Privacy Shield framework.

To be eligible for certification under the DPF, the US company must be subject to the investigatory and enforcement powers of the Federal Trade Commission (FTC) or the US Department of Transportation (DoT),[27] which most companies are. Companies can self-certify online for the EU-US DPF for transfers of personal data from the EEA to the US and register at the same time under parallel frameworks for Switzerland and the UK.[28] US companies are required to re-certify their adherence to the principles on an annual basis.[29]

As part of their certification, companies have to confirm that they have conducted and documented a self-assessment and commit to a set of privacy principles contained in Annex I to the adequacy decision. These principles include purpose limitation[30] and choice,[31] the notice principle,[32] the access principle,[33] the accountability for onward transfer principle[34] and the recourse, enforcement and liability principle.[35] The substantive principles that US companies have to adhere to if they join the DPF are substantially similar to the principles under the EU–US Privacy Shield framework. The CJEU had not expressed concerns regarding these principles. Thus, not much changes for US companies that decide to remain in the programme.

Companies that leave the EU–US DPF have to delete personal data from the EEA that they collected while they were participating in the programme, or find alternative compliance mechanisms. They are then entered on an 'inactive' list, which the US Department of Commerce publishes online next to an 'active' list.[36]

IMPACT OF THE ADEQUACY DECISION REGARDING THE DPF

If a US company registers under the DPF, companies in the EEA can transfer personal data to it as if the US company was based in the EEA and failures to comply with data protection law requirements can be sanctioned not only by data protection authorities in the EEA, but also by the FTC.

Transfers to US companies included in the DPF list

In respect of those US companies that are included in the DPF list maintained and made publicly available by the US Department of Commerce,[37] the US is deemed to ensure an adequate level of protection for personal data transferred from the EU. Thus, companies in the EEA may transfer personal data to a US company included in the list based on the Adequacy Decision. Another transfer mechanism, a data transfer impact assessment (DTIA) or supplementary measures are not required.[38] That means that personal data may be transferred from the EU to the DPF listed US company as if the recipient was located in the EEA — provided that there is a statutory permission and other local data protection law requirements are complied with (Figure 1).[39]

Transfers to US companies not included in the DPF list, but based on other transfer compliance mechanisms

Transfers to companies in the US that are not included in the list, ie that have not certified under the DPF, cannot be based on the Adequacy Decision. They will need to be based on other transfer compliance mechanisms, such as appropriate safeguards pursuant to Article 46 of the GDPR, which include the most common transfer vehicle — the EU SCCs 2021/914.[40]

The question is whether and to what extent the Adequacy Decision impacts the other transfer vehicles. There are good arguments that the Adequacy Decision also has a positive effect in this regard because an essential element of the US legal framework on which the Adequacy Decision is based concerns EO 14086 and accompanying regulations. The Adequacy Decision 'is notably based on the adoption of updated policies and procedures to implement EO 14086'.[41]

As stated in Recital 7 of the Adequacy Decision, the European Commission has carefully analysed US law and practice, including Executive Order 14086 'Enhancing Safeguards for US Signals Intelligence Activities' and the 'Regulation on the Data Protection Review Court' issued by the US Attorney General and based on the findings adopted by the Adequacy Decision. In particular, Recitals 124 to 200 of the Adequacy Decision focus on the change in the legal landscape. The European Commission concludes its analysis, *inter alia*, with the statement that

> when U.S. law enforcement and national security authorities access personal data falling within the scope of this Decision, such access is governed by a legal framework that lays down the conditions under which access can take place and ensures that access and further use of the data is limited to what is necessary and proportionate to the public interest objective pursued. These safeguards can be invoked by individuals who enjoy effective redress rights.[42]

The aspects of clear rules for access and proportionality, as well as effective judicial protection, were the main arguments of the Schrems II decision, which according to the European Commission now seem to have been addressed.

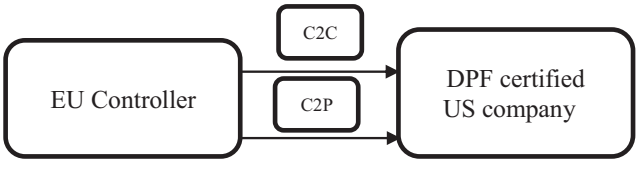

Figure 1: Data transfers to US companies included in the DPF list

In its FAQ regarding the DPF, the European Commission explicitly states:

> All the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transfers under the GDPR to companies in the US, regardless of the transfer mechanism used. These safeguards therefore also facilitate the use of other compliance mechanisms, such as standard contractual clauses and binding corporate rules.[43]

In addition to this, the European Data Protection Board (EDPB) explicitly states:

> In this respect, the EDPB underlines that all the safeguards that have been put in place by the US Government in the area of national security (including the redress mechanism) apply to all data transferred to the US, regardless of the transfer compliance mechanism used. Therefore, when assessing the effectiveness of the Article 46 GDPR transfer compliance mechanism chosen, data exporters should take into account the assessment conducted by the Commission in the Adequacy Decision.[44]

The German data protection conference (consisting of the German data protection authorities) makes a similar statement in its application notes regarding the transfer of personal data from the EU to the US.[45]

Unfortunately, the documents do not contain guidance on what this means for DTIAs. The statement from the EDPB suggests that DTIAs are still required. Companies may find this odd, because most of the potential concerns regarding US government surveillance and other threats to data protection apply regardless of whether a US company registers for the DPF or signs SCCs. Companies that rely on SCCs or BCRs for data transfers to the US should update their DTIAs to reflect the legal developments in the US and the explicit confirmations from the European Commission and the EDPB cited above. However, it is also prudent to monitor developments, since it is likely that the debate around data transfers to the US will continue (Figure 2).

OTHER TRANSFER COMPLIANCE MECHANISMS FOR INTERNATIONAL DATA TRANSFERS UNDER THE GDPR

The GDPR provides for a number of other transfer compliance mechanisms that companies can select to overcome the third hurdle to international data transfers.

SCCs

By far the most common and relevant transfer compliance mechanism is the conclusion of SCCs issued by the European Commission.[46] The SCCs set out 'appropriate safeguards' within the meaning of Article 46 of the GDPR, provided they are not modified except to select the appropriate module(s) or to add or update

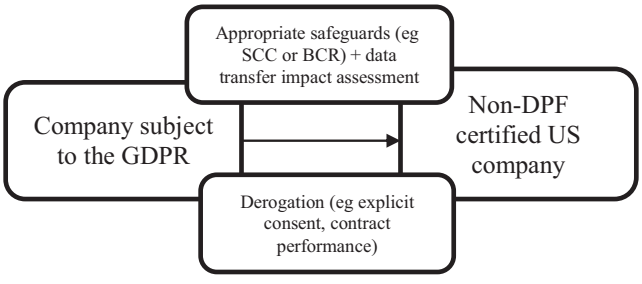

Figure 2: Data transfers to US companies not included in the DPF list

information in the appendix (see clause 2 lit. a). Companies may include the SCCs into a wider contract, provided that they do not contradict, directly or indirectly, the SCCs or prejudice the fundamental rights or freedoms of data subjects. The SCCs provide for not only a module 'controller to controller' and a module 'controller to processor' as the predecessor SCCs, but also a module for data transfers 'processor to processor' and a module 'processor to controller'. With regard to the 'controller to processor' and/or the 'processor to processor' module, they constitute SCCs pursuant to Article 28, paragraph 7 of the GDPR because they contain the rights and obligations of controllers and processors pursuant to Article 28, paragraphs 3 and 4 of the GDPR (see clause 2 lit. a). The SCCs can also be used by data exporters located outside of the EU, eg in case a company is subject to the GDPR due to its exterritorial effect.

BCRs

For intra-group data transfers, companies can also conclude so called BCRs pursuant to Article 47 of the GDPR. BCRs require the approval of the data protection authority, which generally cooperates through the consistency mechanism pursuant to Article 63 of the GDPR. If the competent data protection authority approves the BCRs, the other authorities in the EU are bound. The mandatory content of BCRs is set out in Article 47 of the GDPR. The EDPB has published several documents and guidance in this regard.[47]

Explicit consent or necessity for the performance of a contract

Article 49 of the GDPR provides for derogations for specific situations. For companies with direct contact with data subjects (eg customers), 'explicit consent' or 'contract performance' may be applicable. In its Schrems II decision, the CJEU explicitly referred to the derogations as an alternative transfer compliance mechanism ('. . . the Court notes that, in any event, in view of Article 49 of the GDPR, the annulment of an adequacy decision such as the Privacy Shield Decision is not liable to create such a legal vacuum'[48]). However, the data protection authorities take a restrictive view and state that derogations only apply to occasional data transfers.[49] In addition to that the requirements for consent are quite high under the GDPR. Consent is valid only if it is freely given, specific, informed and unambiguous (Article 4, No. 11, GDPR).

HOW DOES DPF CERTIFICATION COMPARE TO OTHER TRANSFER COMPLIANCE MECHANISMS?

Companies can assess the available options, as discussed above, based on various different criteria, including the following:

Substantive compliance obligations

From the perspective of US companies, substantive obligations with respect to personal data from the EEA often do not differ much depending on the applicable data transfer compliance mechanism. The DPF principles and the SCCs each contain substantive terms that are intended to commit US companies to core principles of the GDPR. Each framework uses different verbiage and nuances, which may affect companies differently depending on their business focus and overall situation, but at their core, each framework seeks to effectuate GDPR rules.

Similarly, Article 47, paragraph 2 of the GDPR contains prerequisites regarding the content of the BCRs. The data protection authority tasked with reviewing and approving an application for BCRs will usually insist on commitments that will be fairly similar to what the GDPR requires.

Recommendations of the EDPB contain details in this regard.[50]

Where companies rely on explicit consent or contractual necessity, they have more flexibility to define their substantive compliance obligations in the contracts, privacy notices and consent forms they provide to the data subjects. But, if they are seeking consent or executing contracts to satisfy GDPR requirements, the companies are additionally subject to the GDPR. Moreover, data protection authorities and courts will refer to GDPR principles as they review the sufficiency of privacy notices, consent forms and contractual safeguards.

Flexibility and configurability

When companies are able to obtain consent or contractual agreements with data subjects, they may have an advantage in that they can tailor the scope of the consent or contract to their particular situation and avoid having to adapt to the more regulated frameworks of the SCCs, the BCRs or the DPF. Consent is required in many events where companies transfer special categories of personal data, a broad range of data listed in Article 9, paragraph 1 of the GDPR as including health data and ethnicity, which can be gathered from most photos showing eyewear and skin colour.

Yet, consent is valid only if consent is freely given, specific, informed and unambiguous (Article 4, No. 11 GDPR). In addition to that, consent can be withdrawn at any time and the data protection authorities set out quite high requirements regarding valid consent.[51] For cross-border transfers outside of the EU consent additionally has to be explicit. Also, the data protection authorities take a restrictive view and apply consent only to occasional data transfers.[52] Some types of businesses do not have any direct relationship with data subjects, and they cannot therefore approach the data subjects with a request for consent, eg cloud, Software-as-a-Service or outsourcing service providers and companies that host data or websites to which others submit information.

Similarly, contractual arrangements with data subjects are not always in place or suited to justify data transfers. Article 6, paragraph 1 lit. b of the GDPR provides a lawful basis for the processing of personal data to the extent that 'processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract'.[53] Also in this regard the data protection authorities take a strict approach (at least in the context of the provision of online services) and require that the processing in question must be 'objectively necessary' for the performance of the contract with the data subject.[54] Similar to Article 6, paragraph 1 lit. b of the GDPR, Article 49, paragraph 1 lit. b of the GDPR requires that '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'.[55] However, as regards derogations in Article 49 of the GDPR in general, the data protection authorities take a restrictive view and apply it only to occasional data transfers.

Geographic coverage

The DPF is very limited in terms of geographic coverage, because it applies only to transfers of personal data from the EEA, UK or Switzerland to the US and onwards. Also, some US companies take the position that they are not subject to FTC and DOT jurisdiction and can therefore not participate in the programme.

Other data transfer compliance mechanisms can apply with respect to transfers from the EEA to any other jurisdiction. Consent and contractual necessity are more or less recognised universally around the world and can be used for data transfers to or from the EEA or other countries.

Companies that rely on SCCs for transfers of personal data from the EEA can use the model clauses promulgated by the EU plus slightly different clauses for Switzerland and the UK. More and more jurisdictions outside the EU are publishing their own separate standard contractual clauses for international data transfers, which multinational enterprises often append to contract templates on dozens or hundreds of pages.

Companies that are subject to the GDPR and rely on BCRs or SCCs for international data transfers have to conduct and document DTIAs and potentially supplementary measures.[56] These have to be jurisdiction and transfer-specific in scope.

Activities coverage

With a DPF self-certification, a US company can present itself as subject to adequate levels of data protection with respect to all kinds of data categories and processing activities, including data processing arrangements for affiliates and unaffiliated customers, intra-group transfers of HR data, consumer information and details of B2B business partner contacts.

With BCRs, companies can typically only cover international data transfers between affiliates, because unaffiliated companies are unlikely to commit to compliance with BCRs at the stage when a company obtains approval from a data protection authority and submits a list of covered entities. In practice, companies in the EEA take comfort in the fact that a business partner has obtained an approval for BCRs, because that demonstrates a significant investment in data protection law compliance and an endorsement from the data protection authority that approved the BCRs. Technically, the BCRs do not usually cover transfers from an unaffiliated entity to a member of the group that is subject to the BCRs or from a group member to an unaffiliated service provider. Also, unaffiliated companies cannot reasonably be expected to commit to BCRs from an unaffiliated vendor or customer, because BCRs tend to be customised to a particular group and cover most or all of its data processing activities, which are likely to be different from those of an unaffiliated customer or vendor.

Companies that rely on consent or necessity for contract performance with data subjects have to specifically address each type of data processing activity, because consent must be specific to be valid and contractual necessities arise only from specific contracts. In practice, consent and contractual undertakings are often not an option in certain scenarios, for example, in the human resources context where consent is deemed coerced or due to a lack of direct contact with data subjects or a business context that does not induce data subjects to grant consent or conclude contracts.

Companies can also use data protection agreements based on the SCCs to legitimise transfers. But the SCCs require a significant amount of detail regarding data processing practices and purposes to be included in appendices. It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role of the parties as data exporter and/or data importer. This may require the completion and signing of separate appendices for each transfer/category of transfers and/or contractual relationship or it may cause many companies to prepare specific agreements for specific scenarios and this in turn can result in a multitude of limited transfer agreements as opposed to one comprehensive set of rules for all geographies and topics. In addition to that the use of standard contractual clauses requires a data transfer impact assessment to be carried out[57] which is quite challenging in practice and the outcome of the same may differ depending on the location of the data importer/recipient.

Implementation process and timing

Consent forms and contractual undertakings are relatively easy to prepare and implement in online click-through scenarios. Implementing data transfer agreements based on the SCCs does not typically take companies a lot of time in the intra-group context, because the content of the contracts is largely prescribed and translations in all major European languages are available. However, companies with many subsidiaries or particularly dynamic corporate structures or decentralised processing activities view the implementation of data transfer agreements as a more significant burden, particularly if local operations are reluctant to execute the agreements. Moreover, getting unaffiliated business partners to sign the forms can be challenging although SCCs are by now widely known and accepted.

The greatest administrative burden is still associated with the implementation of BCRs. Under the GDPR the requirements for BCRs are set out: BCRs must (i) be legally binding, apply to and be enforced by the group of companies, (ii) expressly confer enforceable rights on data subjects with regard to the processing of their personal data and (iii) fulfil certain specifications outlined in Article 47, paragraph 2 of the GDPR (see Article 47, paragraph 1 of the GDPR). The competent data protection authority must approve BCRs in accordance with the consistency mechanism, ie BCRs will formally be recognised across the EU. The competent authority will be the data protection authority of the main establishment (Article 56 of the GDPR). The data protection authorities must cooperate with each other through the consistency mechanism (Article 63 of the GDPR). Although the process is less burdensome than it was before the GDPR (before the GDPR, BCRs required approval from data protection authorities in every EU member state), the approval process of BCRs is still time consuming under the GDPR and beyond a company's control.

However, another challenging burden when relying on SCCs or BCRs is typically the requirement to carry out a data transfer impact assessment.

By contrast, registration under the DPF is relatively easy (online filing only). Nevertheless, US companies will want to take sufficient time before they submit to the DPF, because they need to conduct the required self-assessment and prepare the relevant due diligence documentation in order to be prepared to answer any questions from the Department of Commerce and/or any enforcement actions by the FTC. Such a self-assessment should be undertaken and documented in the context of any of the compliance options. However, companies will have to consider the dynamics and implications of needing a corporate officer to sign a declaration regarding compliance and self-assessment and a possible review process by third party validators or dispute resolution process providers.

Ongoing administration

Consent, contracts and SCCs require action in case of changes (eg additional consent, updating contracts, amending the appendix of the SCCs). For BCRs the same applies, but in addition to that the data protection authorities recommend that the data protection authority should be notified of any changes, with the brief explanation of the reasons for the changes once a year. Article 47, paragraph 2 lit. k of the GDPR requires that the BCRs specify the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority.

The DPF requires annual recertification, but changes in the practical details of data processing do not have to be notified to the US Department of Commerce.

Enforcement risks

The FTC has brought dozens of enforcement actions against US companies

based on alleged failures to comply with the US Safe Harbor Program principles and the EU–US Privacy Shield principles.[58] In a number of cases, the FTC sanctioned companies that claimed to have certified under the programmes without actually registering or who had let their registrations lapse. In other cases, the FTC penalised violations of the respective principles in the context of actions focused also on violations of US privacy laws. US companies that take their obligations under the programmes seriously and comply with formal requirements do not typically fear a significantly increased compliance risk associated with registering for DPF. Yet, many US businesses are concerned that the FTC has been unusually litigious and unpredictable under its current leadership, bringing cases based on novel theories or theories previously rejected by courts.[59]

Regarding SCCs and BCRs, enforcement actions have thus far not been publicised — either in the US or the EU. Companies in the US, however, are concerned about having to submit to the national law and the jurisdiction of EEA member states in the context of SCCs and BCRs.

In respect of consent and contracts with data subjects, enforcement risks tend to depend on a company's exposure to local law and jurisdiction based on its geographic footprint and business posture.

Stability

BCRs offer perhaps the most chance of stability among the data transfer mechanisms. Once a group of affiliated companies obtains approval for BCRs, it should be able to rely on BCRs for its intra-group data transfers.

The EU has updated its SCCs from time to time since it promulgated the first versions in 2001 and 2002. The most recent update in 2021 has been fairly extensive.

The stability of consents and contracts with data subjects depends on the relationship that a company has with its employees, customers and other data subjects. Data subjects can withdraw their consent at any time. Data subjects can typically also terminate contracts.

Whether the DPF enjoys stability depends on the CJEU. Given the Schrems I and Schrems II decisions, and the fact that the latest Adequacy Decision has already been challenged, there is a risk that the DPF will suffer a fate similar to the US Safe Harbor and EU–US Privacy Shield programmes. In addition, the European Commission has to review the Adequacy Decision after one year and subsequently, as per Article 3, paragraph 4 of the Adequacy Decision. The Commission will focus on whether the legal framework applies, including the conditions under which onward transfers are carried out, individual rights are exercised and US public authorities have access to data transferred on the basis of the Adequacy Decision. It is also expected that the Adequacy Decision will be challenged again and, thus, that the CJEU will have to decide whether US law, in particular EO 14086, ensures an adequate level of protection.

Market perception

In its early years, the US Safe Harbor Program offered US companies a way to publicly demonstrate their commitment to data privacy protections and to differentiate themselves competitively. In its final years, so many companies had registered for the US Safe Harbor Program that it became a *de facto* requirement to do business with companies in Europe. Similarly, participation in the EU–US Privacy Shield programme quickly became expected. Whether this will also be the case with DPF remains to be seen. The fact that more 'inactive' than 'active' companies are currently listed may indicate that companies have had enough and are not betting on the third time being a charm.[60]

CONCLUSION

Companies should make their decisions regarding the DPF and other international data transfer compliance mechanisms based on a careful assessment of their jurisdictional footprint, customer expectations, data flows, business needs, risk sensitivities and other aspects discussed in this paper. Compared to the previous programme, the EU–US Privacy Shield, procedural details, enforcement mechanisms and substantive obligations are fairly similar for US companies under the DPF. Whether businesses in the EEA and elsewhere will come to expect DPF registrations as a condition of doing business with US companies remains to be seen; perhaps not, given that many businesses are frustrated with the repeated invalidation of the programmes due to political concerns regarding government surveillance over which businesses have no control. Companies that certify under the DPF will probably have to also sign SCCs and accommodate other compliance mechanisms requested by customers and other business partners. Thus, most companies will consider the DPF as an additional measure not an alternative, which also seems prudent because the Adequacy Decision is already being challenged in the courts and also because most multinational businesses have already implemented standardised data-processing agreements globally.[61] Many US companies that were already enrolled in the previous programmes may prefer to accept automatic enrolment over taking the affirmative steps required to leave the programme, particularly if they have contractually committed to remaining in the programme. Companies in the EEA+ can rely on DPF registration of US companies for international transfers and enjoy benefits where they do; for example, they do not have to conduct or document DTIAs in respect of transfers to companies enrolled in the DPF. If they sign SCCs with US companies instead or additionally, they will continue to be required to conduct and document DTIAs and they should update existing DTIAs to reflect the findings of the Commission in the Adequacy Decision pertaining to DPF.

AUTHORS' NOTE

The authors are partners in Baker & McKenzie's Palo Alto, Frankfurt and Munich offices respectively. This article reflects the authors' personal opinions and not those of Baker & McKenzie, its clients or others.

References and notes

1. European Commission (10th July, 2023) 'Adequacy Decision for the EU–US Data Privacy Framework', available at https://commission.europa.eu/document/fa09cbad-dd7d-4684-ae60-be03fcb0fddf_en (accessed 11th October, 2023).
2. Data Privacy Framework Program (n.d.) 'Data Privacy Framework List', available at https://www.dataprivacyframework.gov/s/participant-search (accessed 11th October, 2023).
3. Commission Decision 2010/625/EU of October 19, 2010 on the Adequate Protection of Personal Data in Andorra, OJ L 277, 21.10.2010, pp. 27–29, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32010D0625 (accessed 11th October, 2023).
4. Commission Decision 2003/490/EC of 30 June 2003 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Argentina, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490 (accessed 11th October, 2023).
5. Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32002D0002 (accessed 11th October, 2023).
6. Commission Decision 2010/146/ of 5 March 2010 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection provided by the Faeroese Act on processing of personal data, available at https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32010D0146 (accessed 11th October, 2023).

7. Commission Decision 2003/821/EC of 21 November 2003 on the adequate protection of personal data in Guernsey, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0821 (accessed 11th October, 2023).
8. Commission Decision 2011/61/EU of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011D0061 (accessed 11th October, 2023).
9. Commission Decision 2004/411/EC of 28 April 2004 on the adequate protection of personal data in the Isle of Man, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32004D0411 (accessed 11th October, 2023).
10. Commission Implementing Decision (EU) 2019/419 of 23 January 2019 pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council on the adequate protection of personal data by Japan under the Act on the Protection of Personal Information, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC (accessed 11th October, 2023).
11. Commission Decision 2008/393/EC of 8 May 2008 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data in Jersey, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32008D0393 (accessed 11th October, 2023).
12. Commission Implementing Decision 2013/65/EU of 19 December 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by New Zealand, available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013D0065 (accessed 11th October, 2023).
13. European Commission (17th December, 2021) 'Decision on the Adequate Protection of Personal Data by the Republic of Korea with Annexes', available at https://commission.europa.eu/document/e9453177-f192-4416-a147-3c57adc468c4_en (accessed 11th October, 2023).
14. Commission Decision 2000/518/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000D0518 (accessed 11th October, 2023).
15. European Commission (28th June, 2021) 'Decision on the Adequate Protection of Personal Data by the United Kingdom — General Data Protection Regulation', available at https://commission.europa.eu/document/dabdaf35-ee58-405e-ac3e-924d04b2cfe4_en (accessed 11th October, 2023).
16. Commission Implementing Decision 2012/484/EU of 21 August 2012 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32012D0484 (accessed 11th October, 2023).
17. 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, available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32000D0520 (accessed 11th October, 2023).
18. Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI identifier: ECLI:EU:C:2015:650, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362 – Schrems I (accessed 11th October, 2023).
19. 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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG (accessed 11th October, 2023).
20. C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] ECLI identifier: ECLI:EU:C:2020:559, available at https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=209021 (accessed 11th October, 2023).
21. At the time of the Schrems II decision, SCCs 2010/87/EU (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, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32010D0087 [accessed 12th October, 2023]) and SCCs 2004/915 (Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004D0915 [accessed 12th October, 2023]) were available.
22. European Data Protection Board (2020) 'Recommendations 01/2020 on Measures That Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data: Version 2.0', available at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (accessed 12th October, 2023).

23. European Commission (25th March, 2022) 'European Commission and United States Joint Statement on Trans-Atlantic Data Privacy Framework', available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 (accessed 12th October, 2023).
24. The White House (7th October, 2022) 'Fact Sheet: President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework', available at https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/ (accessed 12th October, 2023).
25. European Data Protection Board 28th February, 2023) 'Opinion 5/2023 on the European Commission Draft Implementing Decision on the Adequate Protection of Personal Data under the EU-US Data Privacy Framework', available at https://edpb.europa.eu/system/files/2023-02/edpb_opinion52023_eu-us_dpf_en.pdf (accessed 11th October, 2023).
26. US Department of Commerce (3rd July, 2023) 'Statement from U.S. Secretary of Commerce Gina Raimondo on the European Union-U.S. Data Privacy Framework', available at https://www.commerce.gov/news/press-releases/2023/07/statement-us-secretary-commerce-gina-raimondo-european-union-us-data (accessed 23rd October, 2023).
27. European Commission, ref 1 above, Annex I, Section I.2.
28. Data Privacy Framework Program (n.d.) available at https://www.dataprivacyframework.gov, select 'certify now.' (accessed 12th October, 2023).
29. European Commission, ref 1 above, Annex I, Sec. III.6.
30. *Ibid*., Annex I, Sec. II.5.a.
31. *Ibid*., Annex I, Sec. II.2.a.
32. *Ibid*., Annex I, Sec. II.1.
33. *Ibid*., Annex I, Sec. III.8.
34. *Ibid*., Annex I, Sec. II.3.
35. *Ibid*., Annex I, Sec. III.11.
36. Data Privacy Framework Program, ref 2 above; 3766 organisations are showing on the 'inactive' list on September 24, 2023 and 2505 on the 'active' list.
37. *Ibid*.
38. European Data Protection Board (2023) 'Information Note on Data Transfers under the GDPR to the United States after the Adoption of the Adequacy Decision on 10 July 2023', available at https://edpb.europa.eu/system/files/2023-07/edpb_informationnoteadequacydecisionus_en.pdf (accessed 12th October, 2023).
39. As noted earlier in this paper, the DPF concerns only the third hurdle to international data transfers and companies also have to address requirements to overcome the first two hurdles.
40. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj (accessed 12th October, 2023). On June 4th, 2021 the European Commission published new standard contractual clauses with the Commission Implementing Decision 2021/914.
41. European Commission, ref 1 above, Recital 204.
42. *Ibid*., Recital 200.
43. European Commission (10th July, 2023) 'Questions & Answers: EU–US Data Privacy Framework', question 7, available at https://ec.europa.eu/commission/presscorner/detail/en/qanda_23_3752 (accessed 12th October, 2023).
44. European Data Protection Board, ref 38 above.
45. Datenschutzkonferenz (4th September, 2023) 'Anwendungshinweise', p. 31, available at https://www.datenschutzzentrum.de/uploads/dsk/23-09-04_DSK-Anwendungshinweise_EU-US_DPF.pdf (accessed 12th October, 2023).
46. Commission Implementing Decision 2021/914/EU of 4th June, 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, available at https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914&qid=1694976154143 (accessed 12th October, 2023).
47. Eg European Data Protection Board (2022) 'Recommendations 1/2022 on the Application for Approval and on the Elements and Principles to Be Found in Controller Binding Corporate Rules (Art. 47 GDPR)', available at https://edpb.europa.eu/system/files/2023-06/edpb_recommendations_20221_bcr-c_v2_en.pdf (accessed 12th October, 2023).
48. C-311/18, ref 20 above.
49. European Data Protection Board (2018) 'Guidelines 2/18 on Derogations of Article 49 under Regulation 2016/679', available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (accessed 12th October, 2023); European Data Protection Board 'Recommendations 01/2020 on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data', p. 3, available at https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf (accessed 12th October, 2023).
50. European Data Protection Board, ref 47 above.
51. European Data Protection Board (2020) 'Guidelines 05/2020 on Consent under Regulation 2016/679', available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (accessed 12th October, 2023).
52. European Data Protection Board (2018) 'Guidelines on Derogations of Article 49 under Regulation 2016/679', available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_2_2018_derogations_en.pdf (accessed 12th October, 2023).

53. Parliament and Council Regulation (EU) 2016/679 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 (GDPR), available at https://eur-lex.europa.eu/eli/reg/2016/679/oj (accessed 12th October, 2023).
54. European Data Protection Board (2019) 'Guidelines 2/2019 on the Processing of Personal Data under Article 6(1)(b) GDPR in the Context of the Provision of Online Services to Data Subjects', available at https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines-art_6-1-b-adopted_after_public_consultation_en.pdf (accessed 12th October, 2023).
55. GDPR, ref 53 above.
56. European Data Protection Board (2020) 'Frequently Asked Questions on the Judgment of the Court of Justice of the European Union in Case C-311/18 – Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems, available at https://edpb.europa.eu/sites/default/files/files/file1/20200724_edpb_faqoncjeuc31118_en.pdf (accessed 12th October, 2023).
57. See standard contractual clauses, ref 46 above, Clause 14. The requirement to carry out a data transfer impact assessment also stems from the Schrems II decision of the Court of Justice of the European Union as well as from European Data Protection Board, ref 22 above, as well as from Article 5, paragraph 2 of the GDPR.
58. See details explained by the FTC in Annex IV to the DPF Adequacy Decision, ref 1 above.
59. Michaels, D. (12th July, 2023) 'Lina Khan Is Taking on the World's Biggest Tech Companies—and Losing', *The Wall Street Journal*, available at www.wsj.com/articles/lina-khan-is-taking-on-the-worlds-biggest-tech-companiesand-losing-9d8d003e (accessed 11th October, 2023).
60. Data Privacy Framework Program, ref 2 above; 3766 organisations are showing on the 'inactive' list on 24th September, 2023 and 2505 on the 'active' list.
61. Determann, L., Engfeldt, H., Nebel, M., Rebello, F. and Takase, K. (n.d.) 'Standardizing Data-processing Agreements Globally', iapp, available at https://iapp.org/news/a/standardizing-data-processing-agreements-globally/ (accessed 12th October, 2023).