## *Schrems II*: The Noose Tightens

The *Schrems II* decision handed down by the European Court of Justice ("ECJ") on July 16, 2020 creates an acute problem for many companies whose businesses rely on the reliable transfer of personal data to the US from the EU. While there is no "silver bullet" solution, consideration can be given to the following:

- If you relied on Privacy Shield to import personal data from the EU or UK to the US:
    - You must find an alternate route promptly, but continue to comply with Privacy Shield obligations for personal data already imported
    - Alternate options currently available include:
        - Incorporate Standard Contractual Clauses into agreements between data exporters and importers.
        - Adopt Binding Corporate Rules for transfers between affiliates
        - Rely on necessity for transfers related to contract formation or performance.
        - Obtain consent of data subjects if consent can be freely given.
        - Seek approval of Supervisory Authority in country of export for alternative adequate protections, which may include unique contracts or encryption.
        - If all else fails: move processing of EU-origin personal data to the EU or to countries deemed "adequate" such as Canada (for commercial use), Switzerland or Israel.
    - Document your reasons for adopting the new solution or solutions.
    - Amend your privacy policy to reflect the new solution.
- If you did not rely on Privacy Shield:
    - No immediate changes are required
    - But continue to monitor new developments, particularly with reference to Standard Contractual Clauses and Binding Corporate Rules.

A solution will always depend on the specific facts of each data importer, and may well include a combination of the options described above.

A detailed consideration of these options appears below, under "So What Should a US Importer Do?"

**Bulletin**: On July 16, 2020, the European Union's highest court, the ECJ, handed down its long-anticipated decision (the "Decision") in a case[1] with controlling effect on the export of personal data from the EU – especially to the United States. A huge amount of personal data flows from the EU to the US every day, and an immense

[1] Data Protection Comm'r of Ireland v. Facebook Ireland and Schrems (CJEU Case C-311/18 July 16, 2020).

amount of commerce[2] depends on that flow. The Decision is draconian in its effect on US importers of such data, especially those who have relied on Privacy Shield self-certification or Standard Contractual Clauses ("SCC") as the transfer mechanism, and has created an urgent need to find a lawful basis for those transfers. Unfortunately, none of the remaining alternatives are free of risk, and a fully stable solution may await an agreement between the US government and the EU. But what should companies to do in the interim?

**How We Got Here**: The case began when Austrian lawyer-activist Max Schrems asked the Irish data protection supervisory authority (which has jurisdiction over Facebook in the EU) to prohibit transfer to the United States of data he provided to Facebook Ireland. He claimed that US law and practices offered insufficient protection against access to his personal data by the US government. EU law, embodied in the General Data Protection Regulation ("GDPR"), sets out several alternative bases for export of personal data from the EU; export that does not fall within any of those bases is unlawful. The specific issue before the court was whether the EU decision approving SCC should be invalidated. A SCC is a form contract pre-approved by the EU, between exporter and importer, that putatively comprises a lawful basis for export; SCC is the vehicle used by Facebook for transferring personal data from the EU to the US. However, in ruling on the SCC issue, the court also held forth on the validity of another legal basis for export -- "Privacy Shield." Privacy Shield is a uniquely US-oriented framework agreed to in 2016 by the EU and the US; Privacy Shield permitted export of personal data from the EU to US importers who have self-certified to a set of principles that, in essence, incorporate EU data protection law. Some 5,400 US importers relied, many of them exclusively, on Privacy Shield as a vehicle for lawful transfer.

The Advocate General, an expert lawyer who assists the court, recommended in December 2019 that the court simply decide that there was no basis for invalidating SCC, and leave the matter there.[3] But he advised that, should the court probe further, it should invalidate the EU Decision authorizing Privacy Shield. In privacy matters, the ECJ is not known for judicial restraint, and this case proved no exception. The court waded into Privacy Shield and dismantled it, just as it had reached out to dismantle Privacy Shield's predecessor (Safe Harbor) in 2015 when that issue was not specifically before the court.[4] In the matter that was actually referred to the ECJ here, the court found no basis for invalidating the SCC, but that is of little consequence to US importers, as the underlying rationale for invalidating Privacy Shield indicates that, for export to the US, SCC will be of little value.

---

[2] The US Department of Commerce has estimated the annual amount of transatlantic trade as $7.1 trillion.

[3] The court is not required to follow the Advocate General's opinion, and around 20% of the time it does not.

[4] Both the attack on Safe Harbor, and the attack generally on export to the US, emanated in substantial part from the June 5, 2013 disclosures made by Edward Snowden regarding US National Security Agency surveillance.

**The Decision's Rationale**: The court held that data subjects whose personal data is exported under SCC must be afforded a level of protection essentially equivalent to that guaranteed by the EU, *i.e.*, guaranteed by the GDPR read in light of the Charter of Fundamental Rights of the EU, a document of constitutional stature in the EU. That equivalency determination must take into account, not only any contract between exporter and importer, but also relevant aspects of transferee nation government access to the data. The court espoused that the exporter or the national supervisory authority ("SA") in the exporter's country must suspend or prohibit a particular SCC transfer where it concludes that the transfer does not or cannot comply with the SCC, and that EU-level protection cannot be ensured by other means.

Looking to the EU decision approving the SCC, the court concluded that its validity was not called into question merely because the SCC fail to bind the transferee government. But, continued the court, that validity depends on whether the decision includes effective mechanisms rendering it possible in practice to ensure (i) compliance with EU law, and (ii) that export is suspended or prohibited when those clauses cannot be honored. The court then found that the SCC decision did establish such mechanisms: it imposed on both exporter and importer an obligation to verify, before transfer, whether the requisite level of protection is respected in the importer nation; and it required the importer to inform the exporter of any inability to comply with the SCC, after which the exporter must suspend transfer.

After validating the SCC generally, without reference to any particular transferee country, the court turned its attention to Privacy Shield. The court held that the EU decision authorizing Privacy Shield had erred in permitting primacy to US national security, and permitting interference with fundamental rights guaranteed by the Charter. US government access was, in the court's opinion, not circumscribed so as to satisfy the essential equivalence standard under the principle of "proportionality" because government surveillance in the US was not limited to what was strictly necessary.[5] In particular, certain US surveillance programs did not indicate limitations, nor provide data subjects with rights in US courts. Accordingly, the court invalidated the EU's Privacy Shield decision.

**The Underlying Problem**: The court's Decision does not rely on any infirmity inherent in the SCC or Privacy Shield export mechanisms. Rather, it is based on the existence of laws in the transferee forum (the US) that fail to conform to the requirements of EU law. This suggests that, with one possible exception,[6] no matter what export vehicle is used, lawful transfer will not come easy.

---

[5] Numerous studies have shown that US national surveillance law is, on the whole, more privacy-sensitive than the surveillance law of most EU nations.

[6] The exception is appropriate consent. However, consent is unavailable as a matter of law, or difficult to use, in many important situations (*e.g.*, for employee data), and is not feasible in many other situations where it is difficult or impossible to acquire.

**So What Should a US Importer Do?** The GDPR authorizes several export mechanisms but it will be difficult to devise an export scheme that does not, if challenged, involve a risk of running afoul of the Decision, absent an agreement between the US government and EU that resolves the long-term surveillance problem. The following lists each of the export options available under the GDPR, and offers suggestions as to short-term courses of action under each. If you are transferring different types of personal data, you may want to use more than one. Most if not all of these suggestions could well be questioned by an SA , but may nevertheless help to mitigate risk in the event of such a challenge:

- Privacy Shield: If you have been relying on Privacy Shield, you need a new basis – right now. Export under Privacy Shield is no longer viable; it is as dead as Safe Harbor (and for the same reasons). Any data you have that was acquired under Privacy Shield must be maintained in accordance with the restrictions of Privacy Shield for as long as you keep it, or destroyed if destruction is compatible with your contractual arrangements and with law. If you have a written agreement with an EU data controller[7] exporter that references the use of SCCs in the event of a Safe Harbor issue, you should invoke that option and get an appropriate set of SCC executed (if not already done).[8] If you import data from an EU data controller absent such an agreement, you may want to suggest SCCs, perhaps sending a copy with the blanks filled in. By the way, you can incorporate an SCC into another agreement so long as nothing in that other agreement contradicts anything in the SCC. If you import data from an EU processor, there is no set of SCC that applies, but if your attorney can draft a custom agreement with "appropriate safeguards" (see that heading below), and obtain SA approval, that will suffice. Otherwise, an importer from an EU processor will need a legal basis for export other than contractual (see discussion below).
- SCC: For the moment, SCC are viable for export to the US – right up until the exporter or the pertinent SA says they are not The court held that data subjects whose personal data is transferred under SCC must be afforded a level of protection essentially equivalent to that guaranteed by the GDPR read in light of the Charter of Fundamental Rights. With regard to any access by the transferee government, that assessment must consider relevant aspects of the transferee nation's legal system. Unfortunately, the Decision virtually invites the SAs to question the SCC's viability as to certain transferee nations, including the US. But until there is an adverse decision by an SA, SCC is a valid export mechanism. Anyone relying on SCCs should also monitor the positions of various SAs. If the SA in your exporter's Member State suspends or prohibits export to the US from that Member State, consider transferring your data from

---

[7] A "controller" determines the means and purposes of processing.

[8] If you are a controller, use the December 27, 2004 set found at https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:385:0074:0084:EN:PDF. If you are a processor (the party processing on behalf of and on the instructions of the controller), use the February 5, 2010 set found at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010D0087&rid=4.

that Member State to another where the SA hasn't yet reached such a conclusion, and then exporting from that second Member State to the US.[9]

- Binding corporate rules: BCRs are multi-party agreements among affiliates of a single international enterprise that agree to be bound by a set of data protection provisions. A set of BCRs generally needs to be approved by a host of SAs but, unlike the SCC situation, it will be unique, and not as clearly controlled by SA action in other matters as is the case for SCC.
- Necessity: Create an express assertion in your privacy policy or contracts that you are transferring personal data to the US on the ground of a pertinent necessity, which is expressly acknowledged as a basis for transfer in GDPR Article 49. Necessity can arise as an export basis –
    - for occasional transfers, for the performance of a contract between data subject and controller;
    - for occasional transfers, for the conclusion or performance of a contract in the interest of the data subject between the controller and another natural or legal person;
    - for important reasons of public interest;
    - for occasional transfers, for the establishment, exercise or defense of legal claims;
    - to protect the vital interests of an individual, where the data subject is incapable of giving consent; or
    - where no other basis applies and not repetitive, for the controller's compelling legitimate interests not overridden by the data subject's interests.

  Under the principle of proportionality, in challenging a transfer made under any of the necessity justifications, an SA should balance the interests of that necessity against the challenge posed to the fundamental rights of the data subject by the US data protection regime. In particular situations, that analysis might justify a transfer under certain of these necessities, especially necessity for (i) an individual's vital interests, (ii) public interest, and (iii) legal claims. Where any of those apply, it is more likely to succeed than a basis focused on some form of contract. However, the use of the necessity bases is limited as noted above.

- Consent: Explicit, freely given, unambiguous, specific, and informed consent – Consent is often not well suited as a basis for transfer. As a matter of law in some Member States, an individual cannot give consent in a relationship where the individual is at a distinct disadvantage, such as the employment relationship,

[9] There is no guarantee that this would not be considered by some SAs as an export from the first Member State to the US. But, you will have an arguable position, and in the ensuing upsurge of activity, there may be little appetite on the part of an appropriate SA to deal with this matter. Also, even if the transfer between Member States is not considered an export from the EU, it requires a legal basis, which might be difficult to identify in these circumstances.

and in most other Member States such consent has questionable validity. Further, as a practical matter, in many situations appropriate consent is difficult, if not impossible, to obtain. Nevertheless, where it is recognized and can be obtained, and is sufficiently clear, conspicuous, and specific in referencing transfer to a nation not deemed adequate by the EU, consent may be a viable basis for export.

- Appropriate safeguards: Transfer out of the EU is also allowed with "appropriate safeguards." These can in principle be provided by SA-approved custom contracts and privacy policies that provide safeguards for personal data that comply with EU requirements, including the availability of enforceable data subject rights and effective legal remedies. In the context of a transfer from an EU controller to a US data processor the data processing contract required between controller and processor by GDPR Article 28(3) may qualify. Long-term, this solution could well encounter the same fate as SCC because no such contract may supersede US surveillance law, but, in the short term, it may be a viable option. Another safeguard that may qualify as appropriate is encryption in transit all the way to the importer. If interception won't provide useful data to any third party, it is likely that appropriate safeguards have been employed.
- Adequacy: Under GDPR, personal data may be transferred to a country whose laws have been deemed "adequate." Processing in such a country could be an option if the risk of transfer to the US under another rationale is not acceptable and processing in the EU is not an option. Current examples include Switzerland, Israel, and Canada (for transfer in the course of "commercial activities"), but of course not the US.

How long do you have to make changes? It is uncertain. The UK SA (the Information Commissioner's Office – the ICO) has advised: "If you are currently using Privacy Shield please continue to do so until new guidance becomes available." It is unclear whether most SAs share that view. We believe it is unlikely that SAs will immediately begin to investigate and penalize companies that have not yet been able to respond to the Decision. Nevertheless, you should move expeditiously to react affirmatively to the Decision. Develop your plan, start implementing it as soon as feasible, and discuss your intentions with partners and customers.

**Importantly, in any event, after you have made your decision, don't forget to make any necessary changes to your privacy policy, your website, and contracts with your exporters and customers, so as to conform them to your new reality.**

**And What About the UK?** In the wake of Brexit, two issues present themselves regarding the UK.

What law controls export from the UK to the US? *It is, and in the foreseeable future is likely to be, the same as the law controlling export from the EU to the US.* -- Brexit is in a "transition period" presently scheduled to end on December 31, 2020.

Under the Agreement of Withdrawal between the UK and the EU, during this period "the institutions, bodies, offices and agencies of the [European] Union" will apply to the UK and persons within it.[10] "In particular, the Court of Justice of the European Union shall have jurisdiction as provided for in the Treaties."[11] Presumably, during the transition period the GDPR and the Decision apply to export from the UK to the US in the same manner as export from the EU to the US (see above). That covers 2020 and a bit beyond if the transition period is extended. What about thereafter?

The pertinent law is unlikely to be changed between now and the end of the transition period. And on the day after the transition period ends, pertinent UK law will presumably be the same as it was on the last day of the transition period. The GDPR and the UK implementing legislation will still be the law in the UK, as will the Decision. Accordingly, the law regarding export from the UK through end of the transition period and for some time thereafter will be the same as current law regarding export from the EU. See our suggestions above. At some point after transition, the UK may begin enacting new data protection laws, but in our view it is unlikely that those laws will impose new barriers to export.

One wrinkle is that, after transition, UK courts, and not EU courts, will interpret the law. To the extent not controlled by existing EU precedent, UK courts may not view data protection matters in quite the same way that EU courts have.

What is the prognosis for lawful export from the EU to the UK? *Perhaps there is no immediate problem, but in the intermediate term, we believe the situation will be similar to the present EU-to-US situation* – The US and the UK share an unfortunate facet of their law – each has a surveillance statute that irritates continental sensibilities.[12] The US statute – the Foreign Intelligence Surveillance Act - was the basis for the demise of Safe Harbor and, now, Privacy Shield. We believe the UK statute - the Investigatory Powers Act 2016 - will lead to a similar result regarding EU-to-UK transfer.

The UK statute was the focal point of a 2018 decision by the European Court of Human Rights ("ECtHR"), a top European court charged with enforcing the European Convention on Human Rights, another instrument of great import in Europe. That court held that the statute's provision permitting bulk interception of international Internet traffic absent sufficient safeguards violated human rights. Often the ECtHR and the ECJ deal with similar issues, and decisions of each are deemed precedent in the other. Nevertheless, in balancing data protection against other important interests, the ECtHR has been more willing than the ECJ to hold that those other interests prevail. But not this time. This suggests that, since the ECtHR found the UK statute to violate human

---

[10] EU-UK Agreement of Withdrawal, Art. 131.

[11] *Id.*

[12] Again, studies have shown that the US surveillance laws are more privacy-sensitive than the surveillance laws of most EU nations. But EU law does not govern Member State security issues.

rights, then once the issue is presented, the ECJ is quite likely to find that it violates the GDPR and the Charter. And the issue will likely indeed be presented to the ECJ by privacy advocates after the transition period ends. An adverse ruling would put the UK in the same unfortunate box as that in which the US now finds itself.