If your company, like many other US insurance companies, has an EU or UK affiliate or parent, and you transfer personal data to the US, including employee data or even data of US persons, or if your trusted service providers do, the Schrems II European Court decision has seismic significance.

On July 16, 2020, the Court of Justice of the European Union (CJEU) issued its much anticipated judgment in what has become known as the Schrems II case. It struck down the EU-US Privacy Shield, which has limited direct applicability to US insurance companies given its requirement for FTC jurisdiction, but it also left the ongoing viability of “Standard Contractual Clauses” and “Binding Corporate Rules” for transfers to the US in serious doubt. Many insurance companies rely on the SCCs to bring data from the EU to the US, and even wholly US data stored in the EU/UK is impacted.

On July 23, the European Data Protection Board (EDPB) came out with FAQs, which sharpen and clarify the impact of the CJEU’s decision.

**Privacy Shield**

Approximately 5300 businesses rely on Privacy Shield to transfer data from the EU/UK to the US, and while insurance companies rarely use it, their key service providers may. The judgment means that those service providers technically can no longer rely on the Privacy Shield to transfer personal data, including employee data and data of US persons from the EU to the US, effective immediately. Transfers on the basis of this legal framework are “illegal,” according to the EDPB, and there is no grace period. Prior to the release of the EDPB FAQs, there had been a range of responses on this point from EU member state data protection authorities. Some quietly indicated they would exercise what discretion they had in how they initially pursue enforcement to allow solutions to be found, but recognizing that they equally have duties to respond to complaints made. The UK ICO (which is no longer a voting member of the EDPB) for its part advised that it was updating its guidance and in the meantime, those currently relying on the Privacy Shield may continue to do so for their existing transfers, though organizations are advised not to start using it at this time. However, this leniency, if it remains following the EDPB FAQs, is best seen as a deferral of proactive enforcement, not as an indefinite leave to continue using Privacy Shield.

**Standard Contractual Clauses**

If, as is more likely, your business uses the Standard Contractual Clauses (SCCs), the Schrems II judgment means that, for the moment, you may continue to do so; but there is a significant new due diligence piece you must conduct to better ensure that the recipient of your personal data can comply with the
clauses and sufficiently protect the data. According to the EDPB:

Whether or not you can transfer personal data on the basis of the SCCs will depend on the result of your assessment, taking into account the circumstances of the transfers, and supplementary measures you could put in place. The supplementary measures along with SCCs, following a case-by-case analysis of the circumstances surrounding the transfer, would have to ensure that U.S. law does not impinge on the adequate level of protection they guarantee.

What that means is that for transfers to the US, your company will need to analyze and document: (i) whether and how the Foreign Intelligence Surveillance Act (FISA) Section 702, dealing with the collection of the content of communications from non-US persons located outside the US, and the collection of personal data of non-US persons located abroad, or Executive Order (EO) 12333, an authority the Court believes can enable bulk collection of personal data transiting undersea cables, applies to a particular data flow; and (ii) whether the effect of those authorities could be mitigated by, for instance, encrypting data in transit.

Fortunately, the reach of FISA § 702 for insurance companies is likely limited, since it applies to “electronic communications service providers.” However, that is not to say that service providers to insurance companies are not within the reach of FISA § 702 (especially cloud service providers), so it will be important to analyze each relevant data stream, whether employee data, customer data, or claims data.

According to the EDPB, if you come to the conclusion that FISA § 702 and/or EO 12333 apply and the supplementary measures are insufficient, you are "required to suspend or end the transfer of personal data." Interestingly, the EDPB contemplates that you may nevertheless choose to keep transferring data despite this conclusion, and states that if you intend to do so you must notify your competent Supervisory Authority, like the UK ICO. The Supervisory Authority can then audit the continued use of the SCCs and ultimately order it to stop following that assessment.

It remains to be seen whether the EDPB FAQs, and the underlying consistency and cooperation mechanism of the GDPR, of which it is a core part, will in practice create a more consistent approach to decisions on transfers from the Supervisory Authorities going forward. In the immediate wake of the court decision, different views on the viability of the Standard Contractual Clauses were emerging, and these could still yet result in divergence in stance when it comes to considering the cases brought to them. Even with due diligence and supplementary measures, the European court’s Schrems II decision means that individual European data protection authorities can revoke reliance on the SCCs and prohibit or restrict transfers to the US—or to other countries that the EU has not deemed “adequate.” The Irish Data Protection Commissioner, for example, has commented in response to the judgment that the “application of the SCCs
transfer mechanism to transfers of personal data to the United States is now questionable.” A German privacy regulator was even more definitive, declaring the beginning of EU “digital independence,” and advising that the “times when personal data is transferred to the US for convenience or cost savings are over after this judgment.” On the other hand, the UK’s ICO stated: “that it stands ready to support organizations and work to ensure that global data flows continue.”

**Binding Corporate Rules**

This same logic, analysis and way forward for the Standard Contractual Clauses applies to those companies that rely on Binding Corporate Rules to transfer data to the US. As the EDPB explains:

> Given the judgment of the Court, which invalidated the Privacy Shield because of the degree of interference created by the law of the US with the fundamental rights of persons whose data are transferred to that third country, and the fact that the Privacy Shield was also designed to bring guarantees to data transferred with other tools such as BCRs, the Court’s assessment applies as well in the context of BCRs, since US law will also have primacy over this tool.

**Key Takeaways**

Ultimately, if your company wishes to continue to apply Standard Contractual Clauses or Binding Corporate Rules as the solution for existing and new personal data transfers from the UK/EU to other countries like the US, it will be important to: (a) determine the extent to which surveillance authorities apply to the relevant data streams; and (b) assess the level of protection your business, or your service providers and their sub-contractors, can provide for each data stream.

You may also want to distinguish between nice-to-have data transfers and must-have data transfers to limit your risk. In other words, you may want to consider alternatives to storing personal data within, or transferring personal data from, the EU/UK-- which could mean adopting a data localization strategy. In addition, you may want to provide technical measures to safeguard any data sent across borders, especially in transit.

What may be particularly important to the insurance sector is to assess the likelihood of a complaint, particularly from within the workforce when employee data is flowing overseas. While European and UK Regulators lack wide discretion on how to interpret the Court’s judgment, they do have some degree of discretion over how and when to enforce it. That said, regulators are duty bound to respond to complaints, even where they would otherwise not look into a company’s practices. Accordingly, and especially in light of COVID-19 and the business uncertainty it engenders, companies should weigh the risks of a
complaint if they continue to transfer data overseas.

Finally, you may want to consider the so-called derogations (i.e. exceptions) from the restriction on transfer. For example, explicit consent to the overseas transfer of personal data may be an available option, but under the GDPR, consent may be withdrawn at any time and the individual must be informed as to the risks of transfer in the absence of appropriate safeguards. Consent is looked upon very skeptically by EU regulators in the employer-employee context, and it must always be freely given, specific and informed. Other derogations/exceptions include, among others, where it is necessary to perform a contract between the controller and the relevant individual, where it is necessary for conclusion or performance of a contract in the interest of the individual and another person or company, or the transfer is necessary for establishing, exercise or defense of legal claims. The interpretation of when these derogations can be applied has, historically, been quite restrictive so there is some debate as to whether that will be adjusted as further guidance is developed — moving the potential for application more in line with the way such alternative use is referenced by the European court.

Ultimately, all companies, and insurance companies in particular, may want to use this latest, groundbreaking development, to start to generate a broader, overall digital strategy. More seismic privacy and data protection developments will surely come, so the time is ripe to recognize the trends, anticipate the developments, and take proactive measures to future-proof your data practices.

1 “Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems” (Case C-311/18) (Schrems II). The Court found that Privacy Shield framework does not sufficiently protect EU personal data from US national security and surveillance laws that allow access and use of personal data by US public authorities.

2 There is no grace period, according to the EDPB, because “the US law assessed by the Court does not provide an essentially equivalent level of protection to the EU.” https://us.eversheds-sutherland.com/portalresource/20200724_edpb_faqoncjeuc31118.pdf


5 Id.