ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Privacy Shield is Broken

Technology, Privacy, and eCommerce

Recently, the European Court of Justice (CJEU) published its opinion on Schrems II, so named from complaints filed by Max Schrems, an Austrian, against Facebook's transfers of European personal information to the United States. Schrems' complaint is that the personal information transferred to the United States is not adequately protected under EU law, as demonstrated by Edward Snowden who exposed PRISM, a US government surveillance program under the National Security Administration (NSA).

Schrems' first complaint in Ireland in 2013 and the decision by the CJEU in 2015 resulted in the United States replacing the EU-US Safe Harbor Principles with the EU-US Privacy Shield in 2016. Schrems continued to file complaints with the Irish Data Protection Commissioner, and in 2017, the complaints were referred to the CJEU for consideration. This is the Schrems II decision published on July 16, 2020 that companies are now facing.

Key takeaways from the CJEU decision and resulting guidance

US law permits intrusive government surveillance, specifically Section 702 FISA (Foreign Intelligence Surveillance Act) and Executive Order 12333 on United States Intelligence Activities, and applies to any transfer of personal information to the United States via electronic means that falls under the scope of this legislation, and is data transfer mechanism agnostic.

- The EU-US Privacy Shield was deemed inadequate and no longer valid to function as a cross-border data transfer mechanism.
- Standard Contractual Clauses (SCCs) were deemed to still be adequate, but not in isolation. Companies must take an individualized approach.
- The logic for SCCs would equally apply to other data transfer mechanisms, such as Binding Corporate Rules (BCRs), but not to derogations.
- Derogations, such as consent or for reasons of public health, are still valid as supposedly, the data subject has been informed of the risks and/or is aware of the data transfer and lack of adequate protections.

What has happened since July 16?

Various government entities have responded to the decision, but new guidance or determinations are still being issued. For example, the United Kingdom, the EU's General Data Protection Regulation would apply through the transition period, which is scheduled to end on Dec. 31, 2020. Theoretically, the United Kingdom could negotiate data transfer arrangements with the United States independently starting in 2021.

Other European Data Protection Agencies are issuing statements, as is the European Data Protection Board (EDPB) and the European Data Protection Supervisor. Of note, the latter expressed concerns that this was the second adequacy decision by the European Commission that has been overturned in five years, so it is clear that more guidance is warranted. For more information on data transfer mechanisms and adequacy decisions, please see this link. The EDPB has issued FAQs, which do provide information in one easy-to-digest document, but the most important items are the ones confirming that there is no grace period for compliance and that all data transfers to the United States should be assessed individually.

In addition, the US Department of Commerce has issued its own statements and warn that companies that have certified to the Privacy Shield will be held accountable to maintain those

protections. Data that have been transferred pursuant to those certifications must be protected under the same protections, returned to the controller, or destroyed. The European Commission, EDPB, and the US Department of Commerce have indicated that they intend to create a successor to Privacy Shield.

What should companies do?

Although it seems unlikely that trade between the United States and the European Union will come to a halt as it regards personal information, companies should not rely on prior events to guide actions in this one. There is no grace period. SCCs are valid, but not in isolation. If you have BCRs, you should also review individual data transfers.

Here are some steps to take for EU to US data transfers

- Consider retaining your Privacy Shield certification as it is evidence that you do follow a certain level of data protection and should there be a new arraignment negotiated, there will perhaps be a transition plan.
- If you do not wish to retain your certification, follow the provisions to withdraw, including addressing data return or destruction.
- Evaluate all data transfers from the European Union.
- Assess your risk and exposure.
    - GDPR provides for both fines and suspension of processing data.
- Communicate with the data controllers (or data processors depending on your role).
- Review your privacy notice for references to transfers being conducted under the Privacy Shield.
    - You should seek counsel on replacement language, but it may be feasible to state that under the recent ruling, you are currently evaluating data transfers and will update the notice with the appropriate information as soon as possible and make sure there is a clear contact for someone to ask for more information.
- Consider storing European personal information in Europe.
    - Assess whether transfers still occur through remote access.
- Assess transfers from the European Union to other countries as other countries have government mass surveillance laws, such as Australia, Canada, China, India, Israel, New Zealand, Russia, Switzerland, and the United Kingdom.

If you have SCCs in place, review them and the associated data processes carefully to make sure that:

- The SCCs are the right ones for this relationship.
    - SCCs are either EU controller to non-EU / EEA controller or EU controller to non-EU / EEA processor.
    - SCCs do not apply processor to processor.
    - All places where information should be completed on the SCCs are completed correctly.
    - Headers
    - Annex B
- No language has been modified, except additional controls may be added.

Further, the EDPB has declared that they are working on updated SCCs that should be released this

year.

Conclusion

It is clear that the European Union is taking a strong stand on protecting personal information from government intrusion and that the United States is particularly susceptible to restrictions. US companies must take appropriate steps to consider the risk and enact mitigations for personal information being processed from the European Union, and other countries that have similar laws may look to the European Union as a guide for enforcement, just as they have used it as a guide for enacting data protection legislation.

References

Case C-311/18 Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (called “Schrems II”).

Case C-362/14 Maximilian Schrems v Data Protection Commissioner (“Schrems I”), which invalidated the EU–U.S. Data Protection Safe Harbor decision from 2000 (“Safe Harbor”) for the international transfer of personal data.

K Royal

Global Chief Privacy Officer

Crawford & Company

K Royal earned her JD from the Sandra Day O'Connor College of Law at Arizona State University. She also holds a PhD in Public Affairs from the University of Texas at Dallas.

Reach out to K about her column at @heartofprivacy on Twitter, or www.linkedin.com/in/kroyal/.