COVINGTON

EU DPA Enforcement Guidance Post-*Schrems*

February 18, 2016

Data Privacy and Cybersecurity

Industry eagerly awaits further guidance from data protection authorities ("DPAs") relating to the EU-U.S. Privacy Shield as well as on the validity (or otherwise) of other mechanisms for transfers to the U.S., such as standard contractual clauses ("SCCs") and binding corporate rules ("BCRs"). As we explained in recent *InsidePrivacy* blog posts (here and here), publication of an opinion by the Article 29 Working Party, representing, among other things, the EU's data protection authorities, is a key next step that will shape enforcement and data transfer options for companies in the post-*Schrems* environment. Until then, here is a summary of the approach that some of the national DPAs are taking:

- **Austria.** The Austrian Data Protection Authority (the "Austrian DPA") has published FAQs on its website (see here), confirming that data transfers to the U.S. should not take place exclusively on the basis of the Safe Harbor. Instead, companies could either store and process personal data locally on a server in the European Economic Area or in third countries which have been officially recognized as providing an adequate level of protection. Alternatively, they can base the data transfer on one of the statutory derogations or, in principle, on SCCs or BCRs; however, in the latter two cases, the Austrian DPA reserves the right to assess the adequacy of the level of protection on a case-by-case basis in the framework of the authorization procedure. Whilst the Austrian DPA has not stated that it would take enforcement action, it might be obliged to do so if it becomes aware of a violation of the Austrian data protection law.
- **Estonia.** Senior officials within the Estonian Data Protection Inspectorate are reported to have put in place an informal enforcement moratorium, and will not "take enforcement actions against enterprises who were using invalidated Safe Harbor—until the moment when the new EU-U.S. Privacy Shield will be available for them."
- **France.** While the French data protection authority (the "CNIL") is largely aligned with the opinions expressed by the Article 29 Working Party, it has started to implement enforcement measures. We understand that the CNIL started sending notices to data controllers as early as November 2015. The notices remind data controllers that they can no longer rely on the now-defunct Safe Harbor and requested controllers to move to alternative transfer mechanisms. The CNIL had previously stated that if no alternative basis for transfer is declared to the CNIL by the end of January 2016, the CNIL will assume that transfers of personal data to the U.S. have stopped and that the CNIL reserves the right to take appropriate measures if the conditions for transfer of personal data do not comply with the French Data Protection Law.
- **Germany.** The German data protection authorities responsible for data protection at federal and state level (the "German DPAs") published a position paper (see here and our blog post here) on the EU-U.S. Safe Harbor in the wake of its invalidation. Among

other things, the German DPAs announced that the validity of SCCs and BCRs is called into question and that they would not issue new authorizations for transfers to the U.S. based on BCRs or data export agreements (essentially, substantively amended SCCs or ad-hoc agreements). The German DPAs also stated that if they become aware of transfers of personal data exclusively based on the Safe Harbor, they will prohibit such transfers.

This position has also been confirmed in statements issued by individual German DPAs last year and after the public announcement of the Privacy Shield at the beginning of February this year (for instance, for Hessen see here, for Bavaria see here, for North-Rhine Westphalia see here, and for Rhineland-Palatinate see here). Already in November last year, the Hamburg DPA announced a three-phase approach (see here): as a first step, the Hamburg DPA identified companies that are most likely to transfer personal data to the U.S. and informed them of the implications of the *Schrems* ruling; between December 2015 and January 2016 the Hamburg DPA issued information requests to those companies asking them whether they do actually transfer personal data to the U.S. and, if so, on which legal basis; and, as a third step, the Hamburg DPA threatened to take enforcement actions starting in February 2016 to prevent illegal data transfers taking place on the basis of the now-defunct Safe Harbor framework. The most critical position among the German DPAs has been taken by the Schleswig-Holstein DPA (the "ULD"). In a position paper dated October 14, 2015 (see here), the ULD threatened that it may prohibit or suspend data transfers to the U.S. based on the SCCs by administrative order and impose administrative fines for violations of the Federal Data Protection Act. The ULD announced that it will examine whether orders against private bodies must be issued and on which basis data transfers to the U.S. must be suspended or banned. Furthermore, it will examine whether private bodies have committed an offence due to the transmission of data to a third country without an adequate level of data protection.

We are not aware of any of the German DPAs having issued any administrative orders prohibiting or suspending data transfers to the U.S. or imposing sanctions therefore.

- **The Netherlands.** Senior officials within the Dutch Data Protection Authority are reported to be taking a pragmatic, "wait-and-see" approach, noting that it "will not take enforcement actions until we have ended our analysis."
- **Poland.** The Polish data protection authority (Inspector General for Personal Data Protection—"GIODO") released a statement, prior to the Privacy Shield announcement, confirming that under Polish data protection law, SCCs and BCRs can still be used, but that it will "react to any complaints received… even those submitted before 1 February 2016" (the initial end-date of the Article 29 Working Party enforcement moratorium).
- **Sweden.** Senior officials within the Swedish Data Protection Authority are reported to have put in place an informal enforcement moratorium, the duration of which is uncertain as "*for the moment* [the Swedish Data Protection Authority is] not taking any such action" (emphasis added).
- **UK.** The UK Information Commissioner's Officer ("ICO") has said that it is "clear that organisations can continue to use other tools such as SCCs and BCRs for transfers to the USA", and that it is not "rushing to use our enforcement powers. There is no new and immediate threat to individuals' personal data that has suddenly arisen that we need to act quickly to prevent" (see ICO blog post and interim guidance).

We will continue to monitor the respective enforcement positions of the Member State data protection authorities as well as the opinion of the Article 29 Working Party, which we can hopefully expect in the coming weeks.

* * *

If you have any questions concerning the material discussed in this client alert, please contact the following members of our Data Privacy and Cybersecurity practice group:

Monika Kuschewsky	+32 2 549 52 49	mkuschewsky@cov.com
Kristof Van Quathem	+32 2 549 52 36	kvanquathem@cov.com
Mark Young	+44 20 7067 2101	myoung@cov.com
Joseph Jones	+44 20 7067 2193	jjones@cov.com