WILMERHALE

The European Data Protection Board's Second Report on the EU-U.S. Privacy Shield

FEBRUARY 1, 2019

The European Data protection Board ("EDPB"), which is composed of representatives of the national data protection authorities, and the European Data Protection Supervisor, adopted its report on the second annual review of the EU-U.S. Privacy Shield on January 22, 2019. This article provides an overview of the main progress and concerns registered by the EDPB both on the commercial aspects of the Privacy Shield and access by U.S. public authorities to personal data transferred from the EU to the U.S.

Background

In July 2016, the so-called "Privacy Shield" decision by the European Commission ("EC") replaced the EC's 2000 "Safe Harbor" decision, which had been struck down by the Court of Justice of the EU because of concerns relating to national security agencies' processing operations following Edward Snowden's allegations. The EU and the U.S. committed to jointly review the Privacy Shield to assess, on an annual basis, its continued adequacy for the protection of personal data. If the EC considers that the Privacy Shield does not continue to provide such adequacy, it may suspend or even repeal the decision. The EC issued its report on the second annual review of the Privacy Shield on December 19, 2018. The EC's report concludes that the Privacy Shield still ensures an adequate level of protection of personal data, highlighting several improvements and raising less concerns than the EDPB. The EDPB's report follows the second joint annual review and complements the EC's report.

EDPB Views regarding Commercial Aspects of the Privacy Shield: Work in Progress

Progress. The EDPB's report highlights three main areas of progress on the commercial aspects of the Privacy Shield, noting that U.S. authorities took into account many of its findings made in the context of the EDPB's first annual review.

1. Improved Certification Process. The DoC has adapted the certification process to avoid inconsistencies between the Privacy Shield List and the representations made by organizations regarding their participation in this program. The DoC now prohibits a first-time applicant from making public representations and premature references about its participation until the DoC

approves its certification. The DoC has not finalized 100 first-time certifications and 30 re-certifications because the formal requirements set out by the Privacy Shield were not fulfilled. The report notes that there is still room for improvement, though, as there are instances where the due date for renewal shown on the Privacy Shield List has already passed, while the organization is still listed as an active participant.

2. Increased Oversight and Enforcement. The DoC and the U.S. Federal Trade Commission ("FTC") have started to take oversight and enforcement actions on their own initiative.

The DoC conducts "false claims reviews" on a quarterly basis to identify organizations that have started but not finished a (re-)certification process, or that did not submit their annual recertification at all. The DoC has also performed a sweep of 100 organizations, focusing on the accessibility of their privacy policy, their responsiveness and the availability of an independent recourse mechanism. The DoC sent more in-depth compliance questionnaires to 21 organizations that showed minor or more significant peculiarities, such as the absence of response from the point of contact, the absence of a privacy policy, or the provision of incomplete information on processing operations. The DoC moves organizations that do not address the issues it pointed out within 30 days to an "inactive" list and refers such cases to the FTC or the Department of Transportation.

The FTC has 40 lawyers almost exclusively working on privacy issues. In 2018, the FTC brought five Privacy Shield cases against organizations that did not complete their certification, or where the certification had lapsed. In most cases, the organizations failed to verify the deletion or return of personal data transferred under the Privacy Shield or continued to represent that they were self-certified under the Privacy Shield Principles after their certifications had lapsed.

3. Increased Guidance. The DoC has issued further guidance to help EU individuals understand the Privacy Shield and how to exercise their rights. The DoC has also started to issue guidance for businesses to clarify the Privacy Shield's requirements (see the DoC's FAQs on the notion of processor and on the accountability for onward transfer principle).

Remaining Concerns of the EDPB. Despite its statements that there was real progress in 2018, the EDPB mainly raised two concerns.

1. Substantive Oversight. The EDPB considers that the DoC's checks focus on process, such as false Privacy Shield certifications, rather than substance, i.e. whether certified organizations actually comply with the Privacy Shield Principles. For example, the EDPB considers that onward transfers require particular attention. Under the Privacy Shield, the Accountability for Onward Transfer Principle provides that a contract is required when personal data received under the Privacy Shield is transferred to a third-party. The risk is that that third-party processing operations would not be subject to the Privacy Shield Principles. In this respect, the EDPB's report notes its regret that the DoC has not used its right to ask organizations to produce the contracts they have put in place with third-parties to assess whether they provide the necessary safeguards.

Furthermore, the EDPB did not assess the FTC's enforcement actions because the FTC was apparently not able to share substantial information in this respect, for undisclosed reasons.

2. Previously Raised Issues. There are still remaining issues that were already mentioned in the EDPB's first annual review, but which have not yet been addressed. These issues include the absence of key definitions (such as "processor" or "anonymized data"), the need to clarify the application of the Privacy Shield to HR data, the absence of or limitation on certain individuals' rights (i.e. the right to object, the right to access, and the right to be informed for HR processing), and the lack of specific rules regarding automated decision-making having legal effects on individuals or similarly significantly affecting them. However, the EDPB noted in this respect that, according to a study commissioned by the EC, such automated decisions are not taken based on personal data transferred from the EU to the U.S., but rather in situations where a U.S. company directly targets EU individuals. For the time being, this may temper the EDPB's calls to provide for specific rules concerning automated decision making. This, however, is a fast-developing area that authorities will closely monitor in future.

EDPB View Regarding Access by U.S. Public Authorities to Data Transferred to the U.S.: Still Not Facing the Core Issue Despite Progress. The EDPB's report recognizes that some progress has been made regarding access by U.S. public authorities to EU personal data. The EDPB mainly identified two areas of progress.

1. Privacy and Civil Liberties Oversight Board's ("PCLOB") Readiness. Although two remaining positions still need to be filled, the EDPB noted that the appointments of three new PCLOB members, including its chair, enabled the PCLOB to issue its first reports. The PCLOB's mission is to ensure that U.S. intelligence activities are balanced with the need to protect privacy and civil liberties, including the Privacy Shield Principles.

2. More Transparency Surveillance Programs. U.S. authorities have published a report on Presidential Policy Directive 28 ("PPD-28"), which provides principles guiding why, whether, when, and how the U.S. conducts signals intelligence activities. This report clarifies that the PPD-28 is implemented by all intelligence agencies. Also, the U.S. government published several documents, including decisions by the Foreign Intelligence Surveillance Court, to increase transparency about the use of surveillance powers and to help understand how the various surveillance programs, including their safeguards, are operated.

Remaining Concerns of the EDPB. Beyond this relative progress, the EDPB pointed out that three of the main concerns it identified in its first report have still not been addressed.

1. Data Protection v. National Security. The EDPB notes that the U.S. legal framework on collection and access of personal data for national security purposes, especially regarding massive and indiscriminate access, has not significantly changed from the perspective of EU individuals. This is a major issue as this was the reason why the CJEU struck down the Safe Harbor in 2015. Hence the EDPB's report notes regret that the U.S. has not introduced new guarantees for individuals. The EDPB considers that more specific safeguards, such as precise targeting, would be needed instead of generally authorizing surveillance programs. It also encourages the PCLB to clarify how the existing PPD-28 safeguards are applied.

2. Redress Mechanisms. The EDPB pointed out that it is uncertain whether an EU individual could

satisfy the U.S. procedural requirements of standing when bringing a suit against a surveillance measure. Still, the EDPB noted that the interpretation of the notion of "standing" in surveillance matters is evolving, with cases still pending. In addition, the EDPB's report noted concern about the available and effective remedies for individuals in circumstances where personal data processed by companies are accessed by law enforcement authorities.

3. Ombudsperson's Powers. In the EDPB's words, "the Ombudsperson mechanism complements the possibilities of redress, or more critically, it might be argued that it is meant to compensate for the uncertainty or unlikeliness to seek effective redress before a U.S. court in surveillance matters." Considering the Ombudsperson's major role, the EDPB insists that its independence is crucial and that this requires the appointment of a permanent Ombudsperson. The EC also considered this a major issue and said it expected the U.S. government to appoint a permanent Ombudsman by the end of February 2019. On January 18, 2019, the White House announced the U.S. President's intent to nominate Keith Krach to that position. The U.S. Senate has still to approve this nominee. The EDPB also considers that the Ombudsperson's powers are not sufficient, especially because he or she is not in a position to bring a matter before courts.

Conclusion: The EDPB's Position and the Future of the Privacy Shield

The EDPB's position in the context of the Privacy Shield annual review involves a tightrope walk, with the EC and trade objectives on one side, and the CJEU and EU data protection laws on the other. On one hand, the EDPB's report constantly seeks to constructively highlight U.S. progress, rather than focusing on the Privacy Shield's perceived shortcomings. On the other hand, however, the EDPB appears desirous to protect its credibility by raising concerns, albeit always presenting them as areas for improvement rather than as obstacles.

Despite real progress on the commercial aspects of the Privacy Shield, the issue that led the CJEU to strike down the Safe Harbor still looms large as there has been limited significant substantive change regarding the U.S. legal framework on collection and access of EU personal data for national security purposes. The EDPB is certainly aware that this is the key issue. It raised it in its Privacy Shield report, but also in its recent report on the EC's adequacy on Japan (see our blog post), in which it reported concerns regarding the willingness with which Japanese businesses voluntarily share customers' personal data with law enforcement agencies. For the Privacy Shield, the key mechanism for transferring personal data to the U.S. remains at risk from the CJEU, should the court uphold the same uncompromising standards it laid down as a justification for striking down the Safe Harbor, when it will rule upon the Privacy Shield (in pending Case C-311/18). Indeed, the EDPB clearly recalled that "the same concerns [it highlighted in its Privacy Shield report, including the collection of EU personal data for U.S. security purposes] will be addressed by the CJEU […]."

In this light, companies should continue to monitor legal developments regarding the Privacy Shield. For its part, the EDPB confirmed that the Privacy Shield is here and that it is not going anywhere…for now.

Authors

Dr. Martin Braun

PARTNER

martin.braun@wilmerhale.com

+49 69 27 10 78 207

Frédéric Louis

PARTNER

frederic.louis@wilmerhale.com

+32 2 285 49 53

Itsiq Benizri

COUNSEL

itsiq.benizri@wilmerhale.com

+32 2 285 49 87