Data Privacy Detective Podcast – Episode 19 – The EU/U.S. and Swiss Privacy Shield

Apr 26, 2018

Categories:

Blogs
Podcast
Publications
Technology Blog

Authors:

Joseph J. Dehner

Brief history

The 1995 EU Privacy Directive aimed to standardize the protection of personal data within the EU by requiring member states to adopt national laws based on common principles, including broad recognition of the right of individuals in the Union to control use of their personal data. This included provisions to prevent the transfer of personal data outside the EU unless transferees committed, or were required by law in their country, to comply with Europe's approach to personal data privacy. Wholesale transfer of personal data to entities in countries lacking an "adequate" level of legal protection as determined by the EU were prohibited. There is an enormous flow of trade, investment and personnel between the EU and the U.S. Cross-border data flows between the U.S. and Europe are the highest in the world. The EU and U.S. thus have a mutual interest in data privacy's not becoming an impediment to commerce.

In the late 1990's the two governments executed a Safe Harbor Agreement that allowed U.S. companies and organizations to meet EU requirements, and so being approved for receipt of EU personal data. Businesses could sign up for the Safe Harbor with the U.S. Commerce Department and Federal Trade Commission (FTC), which effectively became the enforcer of basic rules required for dealing with EU-sourced data. These rules embraced principles of the EU approach to data privacy but did not insist on strict compliance with every individual detail of each EU member state. About 4,500 U.S. companies joined the Safe Harbor. The FTC took enforcement action against about 40 U.S. companies under the Safe Harbor over more than 20 years – less than 1% of businesses that joined. Some see this as lax enforcement. Others see it as proof that the Safe Harbor worked. Regardless, in 2013 revelations surfaced of U.S. National Security Agency surveillance programs and the

involvement of U.S. telecommunications firms in voluntarily providing personal data to U.S. government sources. In October 2015 the Court of Justice of the European Union (ECJ) invalidated the Safe Harbor as not meeting the essential requirements of EU law.

EU and U.S. officials promptly negotiated a replacement published in February 2016, known as the Privacy Shield, adopted by the European Commission in July 2016. In February 2017 the EU and U.S. entered into the EU-U.S. Data Privacy and Protection Agreement (DPPA), an umbrella pact addressing personal information exchanged by law enforcement agencies. In 2017 the judicial redress provisions of the 1974 U.S. Privacy Act were extended to EU citizens. These measures addressed concerns expressed in the ECJ's Safe Harbor decision. Nonetheless, lawsuits are pending by European privacy advocates aiming to have the ECJ invalidate the Privacy Shield, leaving its future uncertain as of May 2018. An EU group known as the Article 29 Working Party has expressed "strong concerns" that certain commercial and national security aspects of the Agreement are inadequate.

Many substantial U.S. companies have enrolled in the Privacy Shield nonetheless, viewing it as a means of permitting the transfer of data of EU persons, including after the coming into force of the more detailed and comprehensive General Data Protection Regulation (the GDPR) that becomes directly applicable law throughout the EU on May 25, 2018.

What is the Privacy Shield, and what does a U.S. business gain and risk by joining it?

The Privacy Shield requires a U.S. business to self-certify to U.S. agencies that it will meet seven distinct categories of principles when dealing with EU-governed personal data:

- Notice to data subjects (people) about collection and use of their personal information
- Choice of data subjects to approve, disapprove or limit use
- Accountability for onward transfers of data

- Security of personal data
- Data integrity and purpose limitation
- Access of people to their data, and
- Recourse, enforcement and liability

A Privacy Shield supplement adds requirements for handling sensitive data, secondary liability, the role of EU member state data protection authorities, human resources data, pharma and medical products, and publicly available data. A model for arbitrating disputes is included. For the U.S. Commerce Department text of the Privacy Shield principles and supplements (including the similar but separate Swiss Privacy Shield Framework), go to https://www.privacyshield.gov/EU-US-Framework.

If a U.S. business self-certifies that it will comply with these provisions and has conformed its practices to meet Privacy Shield principles, then the transfer of EU personal data to it will generally preclude enforcement by EU data protection authorities. Instead, the U.S. Federal Trade Commission can take action against a U.S. signatory to the Privacy Shield, effectively becoming the U.S. policeman for violations of the EU-stated principles. The FTC has authority to combat unfair trade practices and misleading advertising if a business self-certifies but fails to do what it committed to do.

The obvious gain for a U.S. business in joining the Privacy Shield is to be able to receive and process EU personal data without fear of direct challenge by EU data protection authorities. EU data subjects will retain direct individual enforcement rights under the arbitration or other dispute resolution mechanisms permitted by the Privacy Shield, procedures that can take place in the USA and initially through a business' own system for resolving disputes. A broader benefit is reputational, with the U.S. business able to say that it respects the European approach to data privacy, at least as it applies to EU citizens and residents.

The burden and risks to a U.S. business that joins the Privacy Shield

First, there is a sign-up cost ranging from $250 to $3,250 (based on a company's revenues), along with the substantial effort and expense of adapting business methods and technology to conform to the required principles. This effectively requires a U.S. business to comply with the basic framework of the GDPR, as expressed in the seven categories of principles and the supplements.

Second, a U.S. business will face a home-turf regulator in the FTC and must concede that it has no jurisdictional or venue objection to an FTC enforcement action if the business fails to do what it has self-certified. By contrast, a U.S. business that receives EU-governed personal data, but does not materially offer goods and services to EU residents and does not significantly monitor the behavior of EU residents (the two extraterritorial instances where the GDPR expressly applies to controllers and processors of EU personal data under Article 3(2)), would face minimal risk in being challenged directly by an EU data protection authority. Article 27(1) of the GDPR, for example, requires a non-EU business covered by Article 3(2) to appoint a representative in the EU, but Article 27(2) says that this is not required for "processing which is occasional, does not include, on a large scale, processing of special categories of data…."

Third, a U.S. business must commit to principles that by their nature contain ambiguities, as compared with adopting binding corporate rules or the standard contractual clauses of the EU that are alternative ways to receive EU personal data under the GDPR without resort to the Privacy Shield. Numerous requirements are specified by the Privacy Shield beyond those provided under the invalidated Safe Harbor approach. A summary of new provisions compared to the Safe Harbor is available at https://www.privacyshield.gov/Key-New-Requirements.

A business may join the Privacy Shield without having to comply with every specific provision of the GDPR and all the variations about data privacy available to EU member states. Instead, a Privacy Shield business must comply with its principles and supplements. As one example, the GDPR generally requires "opt-in" consent from persons about how their personal data will be used. The Privacy Shield by contrast requires "opt-in" consent only for

"sensitive information," defined for Privacy Shield purposes as "information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual." For non-sensitive information, the principles require the following:

An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be disclosed to a third party or (ii) to be used for a purpose that is materially different from the purpose(s) for which it was originally collected or subsequently authorized by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.

This requires U.S. businesses to change their web-based and other data systems to be far more specific in stating in plain language what uses will be made of a person's personal data than is prevalent under existing U.S. practice (other than in medtech and fintech), while providing "opt-in" language for sensitive information. And then the U.S. business will need to decide whether to provide this type of consent language only for EU-based persons or to provide it generally to all, regardless of residence.

A U.S. business should balance the benefit from joining the Privacy Shield against the risks and burdens it imposes. Almost 3,000 U.S. companies self-certified to the U.S. Commerce Department under the Privacy Shield by mid-April 2018. Many had been Safe Harbor participants.

EU Data Protection Supervisor Giovanni Buttarelli commented at a March 27, 2018 Summit of the International Association of Privacy Professionals, as reported in Bloomberg Law's International Trade Reporter, that the Privacy Shield may soon become obsolete. He said the Shield was a "short-term solution" to bridge the time between the phase-out of the EU Data Privacy Directive and the coming into force of the GDPR in May 2018. He reportedly said that companies doing business in the EU must comply with the GDPR by then, which will require them to meet the full scope of EU rules about personal data for EU residents. If they do that, this would

entail direct compliance with EU data protection rules without need to resort to the Privacy Shield for data transfer propriety.

A final thought

For businesses located outside the EU, there can be substantial benefit regardless of legal considerations in adopting the essential principles and business practices of EU data privacy rules. The recent Facebook/Cambridge Analytica revelations highlight the reputational risk of being viewed as unfair or unprotective in handling personal data. If businesses outside the EU that receive personal data from EU residents provide a heightened set of protections to them, is it responsible from a business standpoint not to provide similar protections to persons who live outside the EU? How can that be defended or explained from a business standpoint? Perhaps Supervisor Buttarelli is right that the Privacy Shield is a short-term solution, not because the GDPR will supplant it for non-EU businesses, but because data privacy is by its nature global, requiring businesses to consider the adoption of data protection policies and procedures applicable to all individuals regardless of where they live.

For more information, please contact Joe Dehner or any attorney in Frost Brown Todd's Privacy and Information Security Law Practice Group.

View the original article as a Frost Brown Todd Legal Update: Data Privacy Detective Podcast – Episode 19 – The EU/U.S. and Swiss Privacy Shield.

FBT Gibbons