Client Alert | Technology / Data, Privacy & Cyber Security

New deal for transferring personal data from the EU to the US moves a step closer

March 2016

Authors: Detlev Gabel, Daren Orzechowski, Robert Blamires, Tim Hickman

Following the conclusion in early February of negotiations for the Privacy Shield (the replacement for Safe Harbor), the European Commission has published draft documents providing the full detail of the Privacy Shield program. This news is of significant importance to all organizations that transfer personal data from the EU to the US.

On February 29, 2016, the European Commission issued a number of documents that provide important information regarding the details of the proposed EU-US Privacy Shield. In early February, the Commission had announced that the negotiations between the EU and the US had been successfully concluded, and would lead to a new Privacy Shield framework. However, at that stage, the Commission only published a high-level description of the principles behind the Privacy Shield, and did not provide full details. The Commission has now published the following documents:

- a press release summarizing the status of the Privacy Shield and the relevant documents;
- a fact sheet highlighting the most important elements of the framework;
- a 'Q&A' document answering questions that the Commission considers to be important;
- a communication issued by the Commission to the European Parliament and the Council of Ministers of the EU regarding the state of play of transatlantic data flows; and
- a new draft Adequacy Decision which, together with its Annexes, provides the most critical information on the nature of the Privacy Shield and its impact on businesses.

Why does this matter?

EU data protection law demands that exports of personal data from the EU to third countries such as the US can only take place if there is a mechanism to ensure an adequate level of protection in the importing country. Between 2000 and 2015, US organizations could certify to the US-EU Safe Harbor. Personal data could lawfully be transferred from the EU to a certified organization in the US, on the basis that the European Commission had issued an 'Adequacy Decision' declaring that Safe Harbor satisfied the requirements of EU data protection law in relation to international data transfers. However, in October 2015, the Court of Justice of the EU ("**CJEU**") ruled that the Commission's Adequacy Decision regarding Safe Harbor was invalid. Consequently, Safe Harbor no longer provides a lawful mechanism for transferring personal data from the EU to the US. Meanwhile the European Commission and the US government had been negotiating the terms of the Privacy Shield, as a replacement for Safe Harbor.

EU Data Protection Authorities ("**DPAs**") initially stated that, until the end of January 2016, they would not take enforcement action against organizations that were still relying on Safe Harbor. That deadline has now passed, and some DPAs have begun taking enforcement actions against organizations that continue to transfer personal data to the US in reliance on Safe Harbor. For example, the Hamburg State DPA in Germany has recently announced that it is taking action against three international organizations that are still relying on Safe Harbor.

The publication of the abovementioned documents by the Commission is of significant importance to organizations that transfer personal data from the EU to the US, because it provides further information on the requirements that those organizations are likely to have to satisfy if they wish to use the Privacy Shield as a replacement for Safe Harbor. However, it is important to note that the Commission's Adequacy Decision regarding the Privacy Shield is still in draft form, and is subject to further amendment.

What are the key points from the Commission's documents?

How do organizations join the Privacy Shield?

Organizations may join the Privacy Shield by providing the US Department of Commerce with a self-certification submission, signed by a corporate officer and including certain minimum information (e.g., the organization's details; a description of the purposes for which it will use data received under the Privacy Shield; a description of the organization's privacy policy; and so on). To qualify for the Privacy Shield, organizations must:

- be subject to the jurisdiction of either the US Federal Trade Commission ("**FTC**") or the Department of Transportation;
- publicly declare that they will comply with the Privacy Principles (as set out below);
- publicly disclose their privacy policies; and
- fully implement the Privacy Principles (as set out below).

If organizations wish to transfer human resources data, they must indicate this separately in their self-certification submission and include details such as their human resources privacy policy.

The Department of Commerce will maintain an online register of organizations that have successfully certified to the Privacy Shield. Organizations must verify their compliance and re-certify to the Privacy Shield at least annually. Existing Safe Harbor certifications will not be transferred across to the new Privacy Shield register, because the requirements of the two schemes are different. Therefore, all organizations that wish to take advantage of the Privacy Shield will have to prepare a fresh certification submission.

What do the Privacy Principles require?

Like Safe Harbor, the Privacy Shield is based on a number of Privacy Principles that are implemented under US law. US organizations that certify to the Privacy Shield will be obliged to comply with these Privacy Principles. In summary, the Privacy Principles are as follows:

- *Notice*: Organizations certifying to the Privacy Shield must publish certain minimum information on their processing activities (e.g., the types of personal data collected, the purpose of processing, right of access and choice, conditions for onward transfers, and liability). Organizations must also publish their relevant privacy policies (which must reflect the Privacy Shield Privacy Principles, and must include a link to the Department of Commerce's Privacy Shield website and the website of the recourse mechanism the organization provides).
- *Choice*: Organizations certifying to the Privacy Shield must provide suitable mechanisms to:
    - allow individuals to opt out of the disclosure of their personal data to third parties (other than an agent acting on behalf of the organization and appointed in accordance with the Privacy Principles);
    - allow individuals to opt out of the use of their personal data for a "materially different" purpose to the purpose for which the data were originally collected;

- allow individuals to opt out of the use of their personal data for direct marketing purposes; and
- in case of sensitive data, obtain the individual's affirmative express consent (i.e., consent must be obtained on an *opt in* basis for these data).

- *Security*: Organizations certifying to the Privacy Shield must take "reasonable and appropriate" security measures, taking into account the relevant risks and the nature of the data. Where an organization engages a sub-processor, it must enter into a contract with the sub-processor guaranteeing the same level of protection as provided by the Privacy Principles. The organization must also take all necessary steps to ensure that the sub-processor adheres to these obligations and may be liable if it does not.
- *Data Integrity and the Purpose Limitation*: Organizations certifying to the Privacy Shield must ensure that personal data that it processes are limited to the purposes of the relevant processing, as well as being accurate, complete, current and reliable for their intended use.
- *Access*: Organizations certifying to the Privacy Shield must provide individuals with a means by which they can:
  - obtain (without the need for any justification) confirmation of whether that organization is processing personal data related to them;
  - obtain a copy of any such data within reasonable time and without undue restrictions; and
  - correct, amend or delete it if it is inaccurate or has been processed in violation of the Privacy Principles.
- *Accountability for Onward Transfer*: Organizations certifying to the Privacy Shield can only transfer personal data to third parties, for limited and specified purposes, on the basis of a contract, and only if that contract provides the same level of protection as is guaranteed by the Privacy Principles. If the transfer occurs between two controllers within a corporate group, the contract may be substituted by other instruments such as Binding Corporate Rules. The entity that received the personal data under the Privacy Shield remains responsible for ensuring that those data are processed lawfully.
- *Recourse, Enforcement and Liability*: Organizations certifying to the Privacy Shield must provide:
  - mechanisms for ensuring and verifying that the organization complies with the Privacy Principles (as such compliance is a compulsory element of certifying to the Privacy Shield) and for ensuring compliance with its own applicable privacy policies; and
  - mechanisms for providing “effective redress” for EU citizens who raise complaints about the organization’s processing of their personal data. This includes the provision of an independent recourse mechanism, such as a private-sector initiative. The Commission indicates (in Recital 30 of the draft Adequacy Decision) that organizations should respond to such complaints within 45 days.

Limits and safeguards regarding US government access to personal data

The documents published by the Commission provide further detail on a range of measures that restrict access by US governmental agencies to data transferred to the US under the Privacy Shield. In particular, the Commission’s draft Adequacy Decision acknowledges reassurances provided by the US government regarding protections implemented under US law in respect of such access (although, as noted in the Conclusion below, it remains unclear whether these reassurances will prove sufficient).

Redress for EU citizens

The Privacy Shield will be enforced by the Department of Commerce and by the FTC. In some instances, EU DPAs are also granted enforcement powers. There are a number of mechanisms by which the rights of EU citizens are protected and enforced:

- *Direct complaints*: Individuals may complain directly to an organization that has self-certified to the Privacy Shield. As noted above, that organization has 45 days to respond. In the case of complaints against US government agencies, EU citizens have a right of redress under the Judicial Redress Act.
- *Alternative Dispute Resolution*: The Privacy Shield will provide for an Alternative Dispute Resolution mechanism, which will be made available to individuals free of charge. The Alternative Dispute Resolution service providers will work together with the Department of Commerce and the FTC to ensure that complaints made by EU citizens under the Privacy Shield are investigated and resolved.
- *Complaints to DPAs*: EU citizens can complain directly to their local DPA, which is then responsible for working together with the Department of Commerce and the FTC to resolve the complaint. The Department of Commerce will provide a dedicated point of contact point, responsible for receiving and following up on such complaints. If an organization wishes to transfer human resources data, it will have to commit to cooperate with the relevant EU DPAs.
- *The Ombudsperson*: The documents published by the Commission also note that the US government has created an Ombudsperson, who will be responsible for guaranteeing that individual complaints are investigated and that individuals receive independent confirmation that US laws have been complied with or, in the event of a violation, that the violation has been appropriately remedied.
- *The Arbitration Panel*: As a mechanism of last resort, individuals may bring complaints to an independent Arbitration Panel, to be drawn from a pool of at least 20 arbitrators designated by the Department of Commerce and the Commission. The proceedings will be governed by standard arbitration rules to be agreed between the Department of Commerce and the Commission.

Annual joint review mechanism

The Commission will continuously monitor the Privacy Shield framework, and the level of compliance by US authorities with the representations and commitments on which the Commission's draft Adequacy Decision is based. In addition, the Commission and the Department of Commerce will jointly review the efficacy and operation of the Privacy Shield on an annual basis. The Commission is required to submit an Annual Report on the functioning of the Privacy Shield to the European Parliament and the Council of Ministers of the EU. This represents a significantly increased level of oversight as compared to Safe Harbor (which did very little in the way of substantive reviews between 2000 and 2015).

If the Commission concludes that the Privacy Principles are not being enforced, or that the relevant US public authorities are not providing the required level of compliance and protection, the Commission will inform the Department of Commerce, and request that appropriate measures are taken to swiftly address these issues within a reasonable timeframe. If the US authorities fail to address the relevant issues, the Commission may suspend or repeal its Adequacy Decision (effectively removing the lawful basis for transfers of personal data to the US under the Privacy Shield).

What happens next?

The Commission's Adequacy Decision remains in draft form for the moment. The next steps are as follows:

- The Commission will consult with a committee of Member State representatives.
- The Article 29 Working Party (an EU advisory body comprised of representatives of the national DPAs of the EU Member States) will prepare an opinion on the Commission's draft Adequacy Decision. This opinion is crucial, because EU DPAs have the power to investigate the lawfulness of data transfers irrespective of an Adequacy Decision made by the Commission.

- The US government, the Department of Commerce and the FTC will begin taking steps to implement the Privacy Shield framework on the US side, particularly in connection with the monitoring mechanisms and the new Ombudsperson.
- The self-certification mechanism will be made available to qualifying US organizations once the Commission formally adopts an Adequacy Decision in respect of the Privacy Shield.

Conclusion

The Privacy Shield is not a done deal yet. Although the publication of the relevant documents by the Commission has provided helpful clarity, there remains a significant level of uncertainty. In particular, there is no clear timeline by which the Commission's Adequacy Decision will be finalized, and it is not yet clear when the Department of Commerce expects to have the self-certification system up and running. It is also unclear whether the assurances provided by the US government will be sufficient to satisfy the Article 29 Working Party and the EU Member States.

Meanwhile, the enforcement picture across the EU is mixed. Some DPAs (e.g., the UK ICO) have stated that they are unlikely to take enforcement action in relation to transfers of personal data to the US that take place before the Privacy Shield is finalized. Others (e.g., the Hamburg State DPA, noted above) have already begun to take enforcement action. Organizations should therefore consider whether they need to implement an interim data transfer mechanism, in response to the enforcement position taken by the DPAs in the EU Member States, from which they transfer personal data to the US.

Consequently, the transfer of personal data from the EU to the US looks set to remain subject to legal uncertainties for the foreseeable future. Organizations that regularly engage in such transfers should keep a close eye on these developments as they unfold. If the Privacy Shield framework comes into force, it may be advisable to consider certifying early on, as organizations that certify within the first two months after the Privacy Shield's effective date will have additional time (up to nine months after such certification) to bring their commercial relationships with third parties into conformity with the Accountability for Onward Transfer principles set out above.

White & Case LLP
Bockenheimer Landstraße 20
60323 Frankfurt am Main
Germany

T +49 69 29994 0

White & Case LLP
1155 Avenue of the Americas
New York, New York 10036-2787
United States

T +1 212 819 8200

White & Case LLP
5 Old Broad Street
London EC2N 1DW
United Kingdom

T +44 20 7532 1000