DATA SUPERPOWER? A REVIEW OF THE PRIVACY SHIELD DOCUMENTATION

05 April 2016 | London
Legal Briefings

The documentation supporting the proposed new EU-US Privacy Shield has been published by the European Commission.

In the aftermath of the decision of the Court of Justice of the European Union in October last year declaring the US Safe Harbor invalid, the Article 29 Working Party set a deadline of 31 January 2016 for the relevant European and US authorities to agree a new framework for the exchange of personal data between the EU and US for commercial purposes. On 2 February 2016, the EU-US Privacy Shield was announced, although no accompanying documentation was produced. The Article 29 Working Party accordingly set another deadline of the end of February for the European Commission to provide it with a copy of all the Privacy Shield documentation. On 29 February 2016, the European Commission then published the legal texts which will put in place the Privacy Shield should it be approved.

This article sets out some key features of the proposed EU-US Privacy Shield for organisations looking to take advantage of this proposed new compliance method for transatlantic data transfers.

SELF-CERTIFICATION

Like the Safe Harbor regime before it, the Privacy Shield will involve a self-certification mechanism for organisations wishing to benefit from the arrangement. In order to get the benefit of the Privacy Shield, an organisation must: (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the "**FTC**"), the Department of Transportation ("**DoT**") or another statutory body that will effectively ensure compliance with the Privacy Principles as described below (other US statutory bodies recognised by the EU may be included as an annex to the European Commission Adequacy Decision in the future); (b) publicly declare its commitment to comply with the Privacy Principles; (c) publicly disclose its privacy policies in line with these Privacy Principles; and (d) fully implement them.

From a practical perspective, this means that the Privacy Shield, like the Safe Harbor before it, will not be available to all organisations. For example, it will not for the moment be available to financial institutions who are not subject to the jurisdiction of the FTC or DoT.

The Privacy Principles will apply immediately upon certification. However, organisations that certify to the Privacy Shield Framework in the first two months following the Framework's effective date will be given an additional nine months in which to bring their existing relationships with third parties into conformity with the Accountability for Onward Transfer Principle (as described below). Organisations which do not take advantage of this first adopter window will need to be fully compliant from the time they self-certify.

The Department of Commerce ("**DoC**") will maintain a publicly available list of organisations that have self-certified and declared their commitment to adhere to the Privacy Principles (the "**Privacy Shield List**"). The DoC will remove an organisation from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification (as required under the Recourse, Enforcement and Liability Principle).

PRIVACY PRINCIPLES

The Privacy Shield sets out seven privacy principles with which organisations will need to adhere:

- Notice Principle - organisations will be obliged to provide information in "clear and conspicuous language" to data subjects on a number of key elements relating to the processing of their personal data (e.g. type of data collected, purpose of processing, right of access and choice, conditions for onward transfers and liability). This notice must include information regarding the redress mechanisms available to data subjects, including recourse to an independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual.

- Choice Principle - data subjects must be able to object (opt out) to their personal data being disclosed to a third party or used for a "materially different" purpose than the one for which it was originally collected. In the case of sensitive data, organisations must obtain the data subject's affirmative express consent (opt in) to their personal data being disclosed to a third party or used for a "materially different" purpose than the one for which it was originally collected. Opt out/opt in mechanisms must be clear, conspicuous and readily available.

- Accountability for Onward Transfers Principle - any onward transfer of personal data from an organisation to controllers or processors can only take place: (i) for limited and specified purposes; (ii) on the basis of a contract (or comparable arrangement within a corporate group); and (iii) only if that contract provides the same level of protection as the one guaranteed by the Privacy Principles. Where compliance problems arise in the (sub-) processing chain, the organisation acting as the controller of the personal data will have to prove that it is not responsible for the event giving rise to the damage, or

otherwise face liability, although it is not clear from the draft text of the Privacy Shield how this will be tested in practice.

- Security Principle - organisations creating, maintaining, using or disseminating personal data must take "reasonable and appropriate" security measures, taking into account the risks involved in the processing and the nature of the data.

- Data Integrity and Purpose Limitation - personal data must be limited to what is relevant for the purpose of the processing, reliable for its intended use, accurate, complete and current. An organisation may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorised by the data subject.

- Access Principle – data subjects will have the right to access their personal data without justification and subject only to payment of a non-excessive fee. Organisations must respond to any request for access within a reasonable period of time. Data subjects must further be able to correct, amend or delete personal information where it is inaccurate or has been processed in violation of the Privacy Principles.

- Recourse, Enforcement and Liability Principle – participating organisations must provide robust mechanisms to ensure compliance with the Privacy Principles and recourse for EU data subjects whose personal data have been processed in a non-compliant manner, including effective remedies. Organisations must annually re-certify their participation in the framework and must take measures to verify that their published privacy policies conform to the Privacy Principles and are in fact complied with. At a minimum, compliance with this principle should include: (i) independent recourse mechanisms under which individual complaints are investigated and resolved at no cost to the individual; (ii) follow-up procedures for verifying that the attestations and assertions organisations make about their privacy practices are true and that privacy practices have been implemented as presented; and (iii) obligations to remedy problems arising out of failure to comply with the Principles and consequences for such organisations.

From a practical perspective, the seven Privacy Principles go beyond what was required under the old Safe Harbor regime. For example, the requirements for onward transfers and third party contracts in the supply chain and the new recourse mechanisms which have to be in place. This means that organisations will not simply be able to transfer across their old Safe Harbor policies and procedures into the new world of the Privacy Shield. The new Privacy Principles mirror many of the requirements set out in the new EU General Data Protection Regulation and organisations wishing to take the benefit of the new framework will therefore need to evolve and amend their current privacy practices to bring them into line with the new requirements.

Aside from the operational requirements placed upon organisations wishing to self-certify under the new framework, the Privacy Shield also seeks to provide assurances around US national security access to personal data transferred to the US. For the first time, the US has given written assurances, to be published in the federal register, that the access of public authorities for law enforcement and national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. The US makes further assurances that there will be no indiscriminate or mass surveillance of personal data transferred to the US under the Privacy Shield.

NEXT STEPS

There are still several legal steps to be taken before the Privacy Shield can be officially adopted. The Article 29 Working Party is expected to adopt its own opinion on the Privacy Shield at its next plenary session on the 12/13 April. Any such opinion will be influential but not binding on the European Commission. Finally, the framework will need to be adopted by the College of the EU Commission. This could potentially happen as soon as June this year.

Once adopted, the existence of the Privacy Shield would enable organisations in the EU to transfer personal data to organisations on the Privacy Shield List without further regulatory scrutiny. Any such "adequacy decision" adopted by the European Commission under the terms of the current Data Protection Directive, would also remain in force under the new General Data Protection Regulation unless and until amended, replaced or repealed by the European Commission in the future.

However, adoption of the Privacy Shield may not necessarily be the end of the story. Once adopted, the only way to question the validity of the Privacy Shield would be through the Court of Justice of the European Union ("CJEU"). However, given the level of interest and criticism of the Privacy Shield proposals, it seems entirely possible that the whole issue could at some point be referred to the CJEU for consideration. For example, Max Schrems, the lawyer who brought the original case of the US Safe Harbor to the CJEU, has made several criticisms of the proposals, concluding that "there will be a number of people that will challenge this decision if it ever comes out this way — and I may very well be one of them". The uncertainty created by the Schrems decision could therefore very well linger for a long time yet.

To view a copy of the Privacy Shield documentation, please click here.

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

NICK PANTLIN
PARTNER, HEAD OF TMT & DIGITAL UK & EUROPE, LONDON
+44 20 7466 2570
Nick.Pantlin@hsf.com

MIRIAM EVERETT
PARTNER, LONDON
+44 20 7466 2378
Miriam.Everett@hsf.com

DUC TRAN
OF COUNSEL, LONDON
+44 20 7466 2954
Duc.Tran@hsf.com

LEGAL NOTICE