ALERT MEMORANDUM

The EU-U.S. Privacy Shield: Practicalities for U.S. Businesses

August 2, 2016

On August 1, 2016, the U.S. Department of Commerce began accepting applications for certification under the new EU-U.S. Privacy Shield.[1] The Privacy Shield places participants under closer scrutiny from the Federal Trade Commission than was the case under its predecessor, the EU-U.S. Safe Harbor,[2] and introduces new obligations such as liability for onward transfers and the provision of free, independent dispute resolution to data subjects.

In October 2015, the Court of Justice of the European Union in *Maximillian Schrems v Data Protection Commissioner*[3] called into question the legitimacy of thousands of transatlantic data flows by declaring the Safe Harbor adequacy decision invalid. The arrival of the Privacy Shield is therefore a positive step for businesses on both sides of the Atlantic. While the Privacy Shield adequacy decision will, in our view, very likely face challenges, EU data protection regulators have indicated that they will reserve further scrutiny of the Privacy Shield until next year.[4] This memorandum summarizes the key components of the new framework and provides some guidance for U.S. businesses considering registration under the Privacy Shield.

If you have any questions concerning this memorandum, please reach out to your regular firm contact or the following authors:

LONDON
City Place House
55 Basinghall Street
London EC2V 5EH, England
T: +44 20 7614 2200

Colin Pearson
+44 20 7614 2390
cpearson@cgsh.com

Gareth Kristensen
+44 20 7614 2381
gkristensen@cgsh.com

PARIS
12, rue de Tilsitt
75008 Paris, France
T: +33 1 40 74 68 00

Fabrice Baumgartner
+33 1 40 74 68 53
fbaumgartner@cgsh.com

Emmanuel Ronco
+33 1 40 74 69 06
eronco@cgsh.com

ROME
Piazza di Spagna 15
00187 Rome, Italy
T: +39 06 69 52 21

Francesco de Biasi
+39 06 6952 2254
fdebiasi@cgsh.com

BRUSSELS
Rue de la Loi 57
1040 Brussels, Belgium
T: +32 2 287 2000

Christopher Cook
+32 22872137
ccook@cgsh.com

Natascha Gerlach
+32 2 287 2201
ngerlach@cgsh.com

FRANKFURT
Main Tower
Neue Mainzer Strasse 52
60311 Frankfurt am Main, Germany
T: +49 69 97103 0

Thomas Kopp
+49 69 97103 246
tkopp@cgsh.com

[1] Commission Implementing Decision of 12.07.2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (the "**Privacy Shield adequacy decision**").

[2] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbor privacy principles and related frequently asked questions issued by the US Department of Commerce (the "**Safe Harbor adequacy decision**").

[3] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner*, 6 October 2015 ("*Schrems*").

[4] Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, July 26, 2016 (http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf)

I. Introducing the Privacy Shield

Context.

The pivotal judgment of the Court of Justice of the European Union (the "**CJEU**") was the final consequence of a complaint brought by Maximillian Schrems against Facebook in Ireland. Schrems complained to the Irish Data Protection Commissioner that, in light of information leaked by Edward Snowden regarding certain activities of the National Intelligence Service, his personal data was not adequately protected when transferred to the U.S.[5]

The Irish High Court referred two questions to the CJEU: (i) whether a national supervisory authority is bound by a European Commission (the "**Commission**") finding of adequacy and (ii) whether a national supervisory authority should conduct an investigation as to adequacy in light of factual developments since the publication of the adequacy decision. The CJEU held that national supervisory authorities are competent to conduct such investigations and went on to invalidate the Safe Harbor adequacy decision. The CJEU explained that the Commission should have established that U.S. law and practice provides a level of protection for fundamental rights, essentially equivalent to the protection guaranteed within the EU, when assessing the adequacy of Safe Harbor. The CJEU determined that the Commission had undertaken no such investigation with respect to U.S. law, but rather had limited its assessment to the Safe Harbor itself.

In particular, the CJEU noted the following:

- EU law requires that any derogations from data protection law for reasons of national security apply only as is strictly necessary.
- However, U.S. authorities were able to access personal data (1) in a way that was incompatible with the purposes for which it was originally transferred, and (2) beyond what was strictly necessary and proportionate for the protection of national security.
- As a matter of EU law, U.S. legislation could not be considered as limited to what is "strictly necessary" where it allows for the general, mass storage of all personal data transferred from the EU (1) without limitation or differentiation in light of the specific objectives pursued, and (2) without objective criteria being established to limit the access public authorities have to the data and its subsequent use.

Additionally, contrary to the fundamental right to judicial protection under EU law, U.S. legislation provided individuals with no means of redress and no means of requesting that the data relating to them be accessed, rectified, or erased.

CJEU in Schrems:

- "*legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life*."

The Road to Approval by the European Commission.

Following the Schrems judgment, the Privacy Shield was placed on the fast-track; a draft adequacy decision[6] was delivered just over four months later and quickly received in-depth scrutiny by the Article 29 Working Party (i.e., representatives from national data protection authorities across the EU, a representative of the Commission, and the European Data Protection Supervisor, the "**Working Party**"). The Working Party concluded on the whole that while good progress had been made, the draft Privacy Shield adequacy decision was in need of improvement, calling for the Commission to "*ensure the protection offered by the Privacy Shield is indeed essentially equivalent to that of the EU*".[7]

[5] For additional information on the CJEU's decision, please refer to our October 6, 2015 alert memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/news-pdfs/cjeu-invalidates-safe-harbor-impact-on-transatlantic-data-transfers.pdf

[6] European Commission press release of February 29, 2016: *Restoring trust in transatlantic data flows through strong safeguards - European Commission presents EU-U.S. Privacy Shield* (http://europa.eu/rapid/press-release_IP-16-433_en.htm).

[7] Working Party Opinion 01/2016 on EU-U.S. Privacy Shield draft adequacy decision, adopted on 13 April 2016

The Working Party outlined the following key concerns:

- *Overall lack of clarity*. The Working Party noted that the numerous annexes to the decision made it complex and in some places inconsistent. The Working Party suggested including a glossary of terms as well as FAQs.
- *Omission of key data protection principles*. The Working Party indicated that certain "key" data protection principles (including limitations as to the duration and purpose for which data is retained) were not reflected in the draft adequacy decision.
- *Complexity of redress*. The Working Party criticized the complex redress system, considering that it would be difficult for data subjects to navigate. The Working Party recommended that the Privacy Shield allow for EU data protection authorities to represent data subjects before the U.S. authorities.
- *Ombudsperson*. While the ombudsperson mechanism was welcomed, the Working Party questioned the independence of the position and requested further clarity as to its role and powers.
- *Massive and indiscriminate collection of personal data*. The Working Party expressed concern that the possibility of "massive and indiscriminate collection of personal data originating from the EU" was not excluded by the draft adequacy decision. Such data collection, in the opinion of the Working Party, could never be considered as proportionate and strictly necessary in a democratic society.
- *Onward transfers to third countries*. The Working Party expressed concerns that the onward transfer principle was not robust enough and stated that onward transfers should only be permitted where the Privacy Shield's principles would be adhered to by third party transferees. Onward transfers should not be allowed to circumvent EU data protection principles.

(http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf)

The Commission re-entered negotiations with the U.S. representatives to address the Working Party's criticisms. A revised draft was then provided to the Article 31 Committee (a committee made up of representatives of the 28 EU Member States and chaired by a representative from the Commission) for assessment and approval. The revised text of the Privacy Shield includes: (i) limitations on data retention (data must be retained only as is necessary for the purpose for which it was collected and only for so long as is necessary to achieve this purpose); (ii) tighter obligations in relation to onward transfers; (iii) clarifications from the U.S. authorities on their data collection practices, including the requirement to limit the collection of data to what is necessary; and (iv) a revised ombudsperson mechanism, accompanied by clarification of the ombudsperson's independence from the U.S. intelligence services. (See below for further details of the final text.)

The Article 31 Committee (on behalf of the Member States) adopted the Privacy Shield on July 8, 2016. Formal adoption by the Commission followed on July 12, 2016. The Working Party has indicated that it will not challenge the Privacy Shield in its first year.[8] However, the Working Party's first annual review is likely to focus on the perceived weaknesses they have already identified, including (i) the lack of safeguards in relation to automated processing, (ii) insufficient evidence and guarantees from U.S. authorities that they will not practice massive and indiscriminate collection and use of data, and (iii) the inadequacy of the ombudsperson mechanism.

Andrus Ansip, Commission Vice-President for the Digital Single Market:

- *"We have worked hard with all our partners in Europe and in the U.S. to get this deal right and to have it done as soon as possible. Data flows between our two continents are essential to our society and economy – we now have a robust*

[8] Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, July 26, 2016 (http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf)

framework ensuring these transfers take place in the best and safest conditions".[9]

II. Overview of the Privacy Shield

Privacy Principles.

In line with the jurisprudence of the CJEU, the EU-U.S. Privacy Shield is intended to cause certified entities in the U.S. to provide a level of protection for personal data which is "*essentially equivalent*" to the protection afforded to EU data subjects under EU law. The underlying principles for compliance with the Privacy Shield are summarized below. Compliance will be monitored by the U.S. Department of Commerce.

- *Notice*: Organizations who self-certify under the Privacy Shield ("**Participants**") will be obliged to provide information to data subjects concerning the processing of their personal data, including: (i) the type of data collected, (ii) the purpose of processing, (iii) the data subject's right of access, (iv) conditions for onward transfers, and (v) liability for such transfers. Participants must make their privacy policies public. Such policies must reflect the privacy principles and provide links to the Department of Commerce's website, with further details on: (a) self-certification, (b) the rights of data subjects, (c) the independent recourse mechanisms available, (d) the organization's complaints procedure, and (e) a link to the Privacy Shield list.[10] The notice requirement must be satisfied before the individual's data is used for any purpose other than that for which it was originally collected by the transferring organization, or before it is disclosed to a third party for the first time.
- *Data Integrity and Purpose Limitation*: A Participant must ensure that the data it collects is limited to what is relevant for the purpose of processing, reliable for its intended use, accurate, complete, and current. For as long as information is retained, the organization must adhere to the privacy principles. While personal information should only be retained for so long as is necessary to serve the purpose of original collection, processing may continue for longer periods in specific cases, such as archiving in the public interest, journalism, literature, art, scientific and historical research, and statistical analysis. Such retention of data will continue to be subject to the privacy principles.
- *Choice*: Participants must provide data subjects with the opportunity to choose whether their data may be disclosed to third parties or used for a purpose other than that for which it was collected. An "opt-out" is sufficient for such purposes. With respect to sensitive personal data,[11] data subjects must provide affirmative, express, "opt-in" consent where the relevant Participant wishes to disclose the information to a third party or use it for a purpose other than that for which it was collected.
- *Security*: Participants must take reasonable and appropriate measures to protect data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. Organizations should also conclude contracts with their sub-processors which guarantee equivalent protection for the data and ensure that sub-processors implement the privacy principles.
- *Access*: Under the Privacy Shield, data subjects will have the right to view the information a Participant holds about them, for a non-excessive fee, within a reasonable time of making such a request. Data subjects must be able to correct, amend, or delete the information where it is incorrect or has been processed in violation of the privacy principles.

[9] European Commission press release July 12, 2016: *European Commission launches EU-U.S. Privacy Shield - stronger protection for transatlantic data flows* (http://europa.eu/rapid/press-release_IP-16-2461_en.htm).

[10] The Department of Commerce has undertaken to maintain and make available to the public, a list of organisations that have self-certified their adherence to the Privacy Shield principles.

[11] Sensitive personal data includes: medical or health records, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the sexual orientation of the individual.

- *Recourse, Enforcement, and Liability*: In order for the privacy principles to provide real protection for EU data subjects, Participants must provide robust compliance mechanisms and proper recourse for EU data subjects whose personal data has been processed in a non-compliant manner. Participants must, therefore: (i) re-certify annually (demonstrating their continuing compliance with the privacy principles); (ii) have effective redress mechanisms in place which allow individuals' complaints to be investigated and resolved independently, expeditiously, and at no cost to the individual; and (iii) be prepared to cooperate with the Federal Trade Commission (the "**FTC**") or the Department of Transportation (as applicable) which will have powers to investigate and enforce compliance with the Privacy Shield. An individual will also be able to bring complaints before his/her local data protection authority, who will liaise with the relevant Participant on the individual's behalf. Additionally, data subjects have a new right of arbitration under the Privacy Shield, as a final resort.
- *Accountability for Onward Transfer*: Onward transfers (i.e., transfers of personal data from the Participant to a third party, irrespective of where the third party is located) are subject to special rules under the Privacy Shield. The rules prevent the Privacy Shield from being circumvented by unregulated transfers. Participants who wish to transfer personal data to other entities may do so only for limited and specified purposes and in a way that guarantees that the data will have the same level of protection. Organizations may only make such transfers on the basis of a contract which guarantees the privacy principles will be complied with. Importantly, organizations will be liable for the onward transfers they make.

Limited Security Exception.

The Privacy Shield still provides for limited exceptions in the field of national security. Adherence to the privacy principles may therefore be limited (i) where necessary to meet national security or public interest requirements, (ii) where conflicting obligations with the Privacy Shield exist under law, or (iii) if European law or member state law allows for such derogation, provided such exceptions or derogations are applied in comparable contexts. The Privacy Shield emphasizes, however, that organizations should at all times strive to comply with the privacy principles and rely on derogations only where necessary.

Key changes since Safe Harbor – new requirements for Participants.

Broadly, the Privacy Shield places Participants under more robust compliance obligations and requires them to maintain numerous recourse mechanisms for the benefit of data subjects. While organizations that had certified under Safe Harbor will recognize many of the principles, the Privacy Shield introduces several new requirements that will increase the regulatory burden and should be considered by any organization deciding whether to certify.

- *Privacy Shield-compliant privacy policies.* Participants must re-draft their privacy policies in full compliance with the Privacy Shield and make these publically available.
- *Liability for onward transfers*. Participants will now be liable for any transfers they make to third parties. Therefore, they must take reasonable and appropriate steps to ensure that the third parties process personal information in a manner consistent with the Privacy Shield's principles.
- *Ongoing responsibilities.* The Department of Commerce will monitor compliance with the privacy principles and will have the power to remove Participants from the Privacy Shield list where they repeatedly fail to comply. When a Participant is withdrawn from the Privacy Shield list, it will be compelled by the Department of Commerce to return all data transferred under the Privacy Shield. When a Participant's certification lapses, it may retain such data, but it must be maintained in accordance with the privacy principles.

- *Provision of free dispute resolution*. Participants must provide an independent recourse mechanism at no cost to the data subject and be willing to submit to binding arbitration at the request of the individual to address any complaint that has not otherwise been resolved.
- *Cooperation with the Department of Commerce*. Participants must respond promptly to inquiries and questionnaires issued by the Department of Commerce in relation to compliance with the Privacy Shield.
- *Transparency with respect to enforcement actions*. Organizations must make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, if the Participant becomes subject to an FTC or court order based on non-compliance.

Mass and indiscriminate surveillance of personal data.

A central issue in *Schrems* was the U.S. government's ability to access the data of EU citizens held by U.S. entities. In response to this issue, the U.S. intelligence community and the Department of Justice have set out in the Privacy Shield texts an account of the ways in which U.S. authorities use, and prevent the abuse of, the data they collect. In particular, the Privacy Shield sets out the limitations U.S. law places on the collection of information for surveillance, alongside the redress mechanisms available to data subjects under U.S. law.[12] In addition, the Privacy Shield details the U.S. Department of State's intention to establish an ombudsperson mechanism to deal with national security-related queries. The ombudsperson mechanism will allow EU data protection authorities to submit requests relating to U.S. intelligence and security practices, on behalf of EU individuals, where there is concern that such practices may infringe EU rights.[13]

Privacy Shield – a stable way forward?

- *Level of increased regulatory compliance:* It is yet to be seen how proactive the Department of Commerce will be and how burdensome their questionnaires could become.
- *Challenge in the European Courts:* Mr. Schrems, or indeed other activists, may still challenge the Privacy Shield as they did the Safe Harbor.
- *Further Working Party Scrutiny*: As noted above, the Working Party continues to have reservations over the Privacy Shield's adequacy and has indicated that it will conduct a review in a year's time.
- *Brexit:* Organizations collecting personal data in, and transferring it from, the UK to the U.S. will in due course need see what approach is adopted by the UK.
- "*It's the same as Safe Harbor with a couple of additions, and it's going to fail like the one before…It's better than Safe Harbor, obviously, but far from what the ECJ has asked for*." –Max Schrems, Privacy Activist.[14]

III. Next Steps for U.S. Businesses

Certification.

As was the case under the Safe Harbor framework, would-be Participants must self-certify on an annual basis in order to benefit from the Privacy Shield. The Department of Commerce began accepting certifications on August 1, 2016.[15] Certifications must contain at least the following information: (i) name and contact details of the organization; (ii) description of the organization's activities with respect to personal information received from the EU; and (iii) a

[12] Annex VI to the Privacy Shield Decision, *Letter from the Office of Director of National Intelligence*; Annex VII to the Privacy Shield Decision, *letter from the DoJ.*

[13] Annex III to the Privacy Shield Decision, *Letter from Secretary of State John Kerry.*

[14] http://fortune.com/2016/07/11/schrems-privacy-shield/

[15] More information on the Privacy Shield framework and self-certification process can be found on the Department of Commerce's Privacy Shield website: https://www.privacyshield.gov/welcome

description of the organization's Privacy Shield compliant privacy policy.

Before certifying, and making representations of compliance with the privacy principles, organizations should take the following preparatory steps:

- *Establish eligibility*: An organization must fall under the jurisdiction of the FTC or, alternatively, the Department of Transportation in order to participate.
- *Update privacy policies*: Privacy policies must be renewed, in compliance with the Privacy Shield, before the certification process can begin. Organizations must make their policies publically available.
- *Select an independent recourse mechanism*: EU data subjects must have access to an independent recourse mechanism provided by the relevant Participant at no cost. The mechanism should be in place prior to certification. Various private sector programs are compliant with the Privacy Shield's requirements (such as, the American Arbitration Association and the Council of Better Business Bureaus, for example); alternatively, organizations can choose to comply and cooperate with EU data protection authorities (subject to an annual fee).[16]
- *Ensure compliance can be verified*: Participants will be called upon to verify their compliance with the privacy principles and should, therefore, ensure they have the mechanisms in place to demonstrate compliance from the outset.[17] Organizations may self-assess or employ an outside compliance reviewer. Either way, organizations should prepare to keep detailed records as to their implementation of Privacy Shield requirements and be able to make these available on request.
- *Designate a contact person*: Each Participant is required to have a designated contact person for all issues arising under the Privacy Shield. Participants must respond to individuals within 45 days of receiving a complaint.

Participants are liable for the data they transfer onward. Therefore, organizations should bring existing contracts with third parties into compliance with the Privacy Shield framework. Companies that self-certify within two months of August 1, 2016 have up to nine months to address such existing relationships.[18]

Key practical points to consider:

- While the decision to join the Privacy Shield program is voluntary, post-certification compliance with the Privacy Shield principles is enforceable under U.S. law.
- As well as the privacy principles detailed above, Participants must comply with the supplementary principles set out in the Privacy Shield. The supplementary principles set out a number of additional requirements covering, for example, sensitive data, journalistic exceptions, and secondary liability. The supplementary principles also provide additional detail on the main privacy principles under the Privacy Shield.
- Non-EU businesses should be aware that they may be subject to EU data regulations even though they do not have a presence in the EU. Under the new General Data Protection Regulation, the location of the "data subject" is the determining factor. The GDPR regulates the transfer of data from the EU to third countries such as the U.S. and failure to comply with the GDPR can give rise to fines of up to up to 4% of

[16] Annex II to the Privacy Shield Decision, Part III, Supplementary Principles, para.5 "*The Role of the Data Protection Authorities*".

[17] Annex II to the Privacy Shield Decision, Part III, Supplementary Principles, para.5 "*Verification*".

[18] Annex II to the Privacy Shield Decision, Part III, Supplementary Principles, para.6 "*Self-Certification*".

global revenue or EUR 20,000,000, whichever is higher.[19]

- Organizations should consider whether data flows sufficiently warrant self-certification under the Privacy Shield framework or whether their existing arrangements provide adequate protection, particularly given that the Privacy Shield will be reviewed in a year's time. However, organizations that were Safe Harbor certified will, in our view, wish to consider reliance on the Privacy Shield as alternative arrangements may come under scrutiny at some point in the future.

…

CLEARY GOTTLIEB

[19] For additional information on the GDPR, please refer to our May 13, 2016 alert memorandum: https://www.clearygottlieb.com/~/media/cgsh/files/alert-memos/alert-memo-pdf-version-201650.pdf.