JONES DAY | One Firm Worldwide℠

WHITE PAPER

March 2015

EU and U.S. Release Terms of Privacy Shield

Stronger and more comprehensive than the 15-year-old Safe Harbor program it replaces, the new EU–U.S. Privacy Shield applies more stringent protection standards to U.S. companies obtaining personal data and information from Europeans. Among other obligations, a U.S. company must publicly declare its compliance with the Privacy Shield's Privacy Principles, provide a mechanism for opting out when a data subject's information might be used for certain purposes, and obtain a data subject's explicit consent prior to sharing sensitive data with a third party.

The Privacy Shield's implementation remains months away, but companies contemplating transitioning to its provisions should immediately begin work on making their data privacy practices compliant.

TABLE OF CONTENTS

The European Commission ("EC") and U.S. Department of Commerce ("DOC") recently released the full text of the EU–U.S. Privacy Shield framework. This release follows the February 2, 2016, announcement that EU and U.S. officials had reached an agreement to replace the recently invalidated Safe Harbor program (the "Safe Harbor") with a more robust and comprehensive transatlantic data transfer scheme.[1]

The details of the Privacy Shield were released as part of a 128-page package that includes an enumeration of the Privacy Shield Principles (the "Privacy Principles"), the terms of the new "Arbitral Model" that will be used to address certain unresolved data protection claims, and letters from various U.S. regulators.[2] The EC also released a draft "adequacy decision" concluding that the Privacy Shield ensures an adequate level of protection for personal data transferråed under its ambit and meets the standards of Directive 95/46/EC (the "EU Directive").[3] Although the draft adequacy decision did not conclude as such, it can be legally assumed that the Privacy Shield meets the standards of the General Data Protection Regulation ("GDPR"), which will replace the EU Directive in two years after it is adopted. In particular, the EC emphasized the strengthened Privacy Principles, the increased transparency obligations imposed on participating companies, the new oversight and recourse mechanisms, and commitments from the U.S. government that surveillance will be limited to what is strictly necessary.

The Privacy Shield is the result of lengthy negotiations between EU and U.S. policymakers aimed at developing an alternative to the Safe Harbor, in which more than 4,000 U.S. companies participated in order to receive personal data from the EU. In October 2015, the European Court of Justice ("ECJ") issued a decision invalidating the EU Commission decision underlying the 15-year-old Safe Harbor. The ECJ concluded that the Safe Harbor failed to provide an adequate level of protection to personal data transferred from the EU to the U.S., largely due to concerns regarding the U.S. government's ability to access transferred personal data as well as the lack of judicial redress afforded to EU citizens.[4]

The new Privacy Shield maintains the annual "self-certification" system of the Safe Harbor. However, companies signing onto this voluntary framework must now certify their adherence to stricter, more extensive Privacy Principles, while also submitting to more robust transparency obligations and oversight mechanisms. A detailed overview of the new framework and its Privacy Principles is discussed below; however, the following highlights some of the key aspects of the Privacy Shield to which companies will be expected to adhere:

- **Publicly declare compliance** with the Privacy Shield's Privacy Principles (discussed below) and publish their privacy policies that reflect the Privacy Principles;
- **Provide a suitable mechanism for data subjects to opt out** if an organization plans to (i) disclose their personal data to third parties (other than processors/agents acting on the organization's behalf), (ii) use their personal data for a materially different purpose than for which it was originally collected, or (iii) use their personal data for direct marketing purposes;
- **Obtain data subjects' express consent** before sharing their sensitive data with third-party recipients or using their sensitive data for a materially different purpose than for which it was originally collected;
- **Execute contracts with third-party processors** obligating them to process data only for limited and specified purposes;
- **Develop policies to ensure that third-party processors handle personal data** in accordance with the Principles and to correct any unapproved processing;
- **Have in place reasonable and appropriate data security measures** that take into account the relevant risks and nature of the data;
- **Provide a suitable mechanism for data subjects to access their personal data** and the ability to correct, amend, or delete such data; and
- **Establish a mechanism for organizations to respond** within 45 days to complaints lodged by data subjects regarding their personal data.

PRIVACY PRINCIPLES

Under the Privacy Shield's self-certification system, organizations must commit to a largely familiar set of Privacy Principles adopted from its Safe Harbor predecessor. The Privacy Shield, however, elaborates upon and strengthens the obligations contained in several Privacy Principles. In particular, organizations must commit to the following:

Notice. The Privacy Shield greatly expands the certifying organizations' obligation to notify individuals about their data

collection practices. For example, organizations transitioning to the Privacy Shield must revise their privacy policies to notify individuals of new details, including, *inter alia*,

- Whether the company is subject to the investigatory and enforcement powers of the FTC or other U.S. agencies;
- That it will adhere to an independent dispute resolution body to address individual complaints;
- The right of individuals to invoke binding arbitration against the company under certain circumstances;
- Its obligation to disclose personal data to public authorities in compliance with lawful requests; and
- Its responsibility and potential liability in cases of onward transfers to third parties.

Organizations must also make public their newly revised privacy policies, which must address and reflect the framework's Privacy Principles, while also providing individuals with links to the DOC's Privacy Shield website, the list of participating organizations the DOC publishes, and the website of the independent dispute resolution provider the organization utilizes. Because most consumer-facing U.S. organizations will comply with the Notice Privacy Principles through their online privacy policies, those companies seeking to participate in the Privacy Shield will need to revise their policies to reflect these new changes. Even if participating organizations do not collect consumer personal data, companies seeking to transfer their HR data or other non-customer data via the Privacy Shield must still comply with the publication requirement.

Choice. In addition to the enhanced notification requirements, participating organizations also must implement mechanisms that provide data subjects with varying levels of choice regarding the use and disclosure of their data. Organizations must offer data subjects the opportunity to *opt out* if the company plans to: (i) disclose their personal data to third parties (other than processors/agents acting on the organization's behalf); or (ii) use their personal data for a materially different purpose than that for which it was originally collected.

In the employment context, EU employers are ultimately responsible, under relevant national law, for providing their employees with choice when *collecting* their personal data. Once a U.S. organization has received employee data from the EU under the Privacy Shield, that participating organization may disclose it to a third party or use it for a different purpose only in accordance with the Choice and Notice Privacy Principles.

Organizations also must obtain individuals' "explicit" (i.e., *opt-in*) consent before disclosing their sensitive data to any third parties (including processors) or using their sensitive data for a materially different purpose. While there was some ambiguity with respect to the definition of "sensitive data" under the Safe Harbor, the Privacy Shield adopts the EU Directive's broad definition of "sensitive data."[5] Thus, a data subject's affirmative, explicit consent is required, absent certain limited conditions, including, *inter alia*, when the processing of sensitive data is in the vital interests of the data subject or another person, necessary to establish legal claims or defenses, or required to provide medical care or carry out an organization's employment law obligations. Lastly, special rules apply to direct marketing, which generally allow data subjects to opt out at any time from the use of their personal data.

Accountability for Onward Transfers. The Privacy Shield tightens the permissible conditions for onward transfers to any third parties and holds self-certified organizations responsible for the conduct of their third-party processors/agents. Unlike the Safe Harbor, participating companies must now enter into contracts with third-party data recipients—whether that party is a separate data controller or a data processor (vendor)—obligating them to process data only for limited and specified purposes and to provide the same level of protections guaranteed by the Privacy Principles. The Onward Transfer Principle also effectively requires mechanisms for oversight of third-party processors by requiring participating organizations to: (i) take steps to ensure the processor handles the data in accordance with the Privacy Principles; and (ii) remediate any unauthorized processing by the processor.

Participating organizations now face potential liability for the processing actions of their processors (and sub-processors) unless organizations can prove they were not responsible for any damaged caused. Organizations should also be prepared to make available summaries or copies of the relevant privacy provisions in their contracts to the data subjects or the DOC upon request.

The Privacy Shield provides a carve-out for the "occasional employment-related operational needs" of a participating U.S. organization, "such as the booking of a flight, hotel room, or insurance coverage." In these situations, Privacy Shield

companies need not enter into a contract with the third-party controller for transfers of data of a small number of employees (as is otherwise required by the Onward Transfer Principle), provided that the company complies with the Notice and Choice Privacy Principles.

Security. As they did in compliance with the Safe Harbor predecessor, organizations will need to demonstrate that they have in place "reasonable and appropriate" data security measures.

Data Integrity and Purpose Limitation. As noted above, organizations must ensure that data is (i) relevant and reliable for its intended purpose, and (ii) accurate, complete, and current. Absent consent, an organization may not process personal data in a way that is incompatible with the purpose for which it was originally collected or subsequently authorized by an individual.

Access. Organizations must implement mechanisms that provide data subjects with (i) access to the personal data processed about them, and (ii) the ability to correct, amend, or delete their personal data where it is inaccurate or has been processed in violation of the Privacy Principles. In the employment context, EU employers will typically provide such access as is required by law in their home countries, regardless of the location of the data. However, the Privacy Shield nonetheless requires participating U.S. organizations processing such data to cooperate with the EU employer in providing employees with access to their data.

Recourse, Enforcement, and Liability. This new Privacy Principle requires robust mechanisms to ensure compliance with the Privacy Principles and afford recourse to EU citizens whose personal data was processed in violation of the Privacy Principles. In particular, as more fully described below, organizations will be required to appoint an independent dispute resolution body that can resolve individual complaints, provide appropriate recourse, and even sanction noncompliant organizations.

As a practical matter, participating organizations must not only self-certify their compliance with these Privacy Principles but must also meet annual verification requirements either through self-assessment or outside compliance reviews. Under the self-assessment approach, organizations must attest in writing that their published privacy policies on EU personal data are accurate and have been fully implemented and that the company meets other obligations, including employee training on the privacy policies. Alternatively, organizations may elect to engage a third party to verify their compliance with and implementation of their published privacy practices, through auditing, periodic checks, or use of technology tools where appropriate. In either case, organizations must be prepared to supply their written verification statements to the DOC or EU data subjects upon request.

INDIVIDUAL REDRESS AND OVERSIGHT MECHANISMS

The new Privacy Shield requires participating organizations to put in place an effective redress mechanism for EU data subjects to lodge complaints directly with the organizations. The Privacy Shield specifically requires companies to establish a contact—either within or outside the organization—that will respond to any received complaint within 45 days and provide an assessment of the merits of the complaint and the actions taken to resolve it.

Most notably, organizations must designate an independent dispute resolution body that will not only be able to investigate and resolve individual complaints and provide appropriate recourse, but also sanction noncompliant organizations in a way that either provides for a reversal or correction of the noncompliant behavior or requires the termination of further processing and/or deletion of the personal data. If the organization fails to comply with the ruling of a dispute resolution body, the body must report this noncompliance to a U.S. authority with jurisdiction (e.g., the DOC and FTC) or a competent court.

Beyond the independent dispute resolution procedure discussed above, organizations are further required to respond to inquiries and other requests for information from the DOC, and possibly EU national data protection authorities ("DPAs"), relating to their adherence to the Privacy Principles. In this regard, participating entities must retain all records related to their implementation of the Privacy Principles and their privacy policies and make them available upon request of a government agency or independent recourse body in the context of an investigation or complaint about noncompliance.

Moreover, the DOC will conduct compliance reviews of self-certified organizations—including by sending detailed questionnaires—to verify that companies' privacy policies and

practices conform to the Privacy Principles. In addition to general compliance assessments, these reviews will also be undertaken in response to specific complaints or when there is evidence that a participating organization is not complying with the Privacy Principles. Also, the Privacy Shield will allow EU data subjects to raise complaints of noncompliance by participating U.S. organizations directly with their national DPA, which can then channel those complaints to the DOC. Through this special procedure, the DOC will follow up with companies to facilitate resolution and liaise directly with the referring DPA on ongoing compliance issues.

Perhaps most remarkably, the Privacy Shield requires participating U.S. organizations to submit directly to the jurisdiction of foreign DPAs under certain circumstances. Specifically, when an EU citizen refers a complaint to his or her national DPA regarding noncompliance with the Privacy Principles, U.S. participating organizations are obligated to comply with the DPA's investigation and resolution of the complaint if: (i) it concerns processing of human resources-related data collected in the context of the employment relationship; or (ii) the company has otherwise voluntarily submitted to oversight by DPAs under the Privacy Shield.

In particular, these companies will be required to respond to any DPA inquiries, comply with advice given by the DPA (including remedial and compensatory measures), and provide the DPA with written confirmation of compliance with DPA orders. The inquiries and advice will be handed down by an informal panel of multiple DPAs in order to promote a more unified approach to compliance. The panel is expected to deliver advice within 60 days of receiving a complaint; if a company fails to comply with this advice within 25 days and has offered no satisfactory explanation for the delay, the panel will either (i) submit the matter to the FTC (or other competent authority) for a possible enforcement action, or (ii) inform the DOC that there has been a persistent failure to comply with the Principles, in which case the organization will be removed from the Privacy Shield.

Importantly, as highlighted by the ECJ when it invalidated the Safe Harbor, the Privacy Shield text also makes it clear that a DPA is entitled to *suspend* certain data transfers if it believes that an EU citizen's personal data transferred to an organization in the U.S. is not being afforded adequate protections. Moreover, even if a DPA to which a complaint has been addressed does not take any action where a complaint has been lodged, the individual data subject may challenge the DPA's decision (or lack thereof) in the national courts of his or her EU Member State.

Participating organizations also can expect increased FTC enforcement actions under the Privacy Shield. Past Safe Harbor-related enforcement actions were mainly limited to companies that continued to reference their participation in the Safe Harbor despite a certification that had lapsed. Under the Privacy Shield, the FTC will create a standardized referral process that gives priority consideration to referrals of non-compliance by independent dispute resolution bodies (or self-regulatory bodies), the DOC, and a relevant DPA (whether acting on its own initiative or upon individual complaints). The FTC will also accept complaints *directly from individuals*. Following an enforcement action, any settlement between the FTC and a Privacy Shield organization must include mandatory self-reporting provisions, and organizations will be required to make public any Privacy Shield-related compliance reports or assessments submitted to the FTC.

Finally, as a mechanism of "last resort," when an individual believes that none of the other available methods of redress have satisfactorily resolved his or her complaint, an EU data subject may compel a Privacy Shield-participating organization to submit to binding arbitration in the U.S. in front of a Privacy Shield Panel. The parties will be allowed to select a panel of one or three arbitrators from an available pool of arbitrators designated by the DOC and the EC. This Privacy Shield Panel will have the power to impose equitable (non-monetary) relief to remedy noncompliance with the Principles, and all decisions by the Panel will be enforceable by U.S. courts in the event a company fails to comply with its ruling. It should be noted, however, that arbitration may *not* be invoked against companies that have submitted to the jurisdiction of the relevant DPA—namely, those organizations that have either voluntarily committed to cooperating and complying with the advice of a DPA or are obligated to do so with respect to the processing of HR data collected in the employment context.

INCREASED TRANSPARENCY

The DOC aims to be more rigorous in identifying companies that are noncompliant with the new framework's provisions and the self-certification requirements. As with the Safe Harbor, the

DOC will make available a list of self-certified organizations. However, unlike the Safe Harbor, the DOC will: (i) publish a record of entities that have been removed from the list, along with the reason for such removal, and (ii) provide a link to a list of Privacy Shield-related FTC enforcement actions and cases, which will be maintained on the FTC website.

Further, when an organization is no longer a member of the Privacy Shield (e.g., voluntary withdrawal or failure to recertify), the DOC will be responsible for monitoring the organization to:

- Ensure it has deleted any public statements to the Privacy Shield that imply its continued participation;
- Refer the matter to the competent authority (e.g., the FTC) for possible enforcement actions if such organization continues to make false claims; and
- Verify, through use of questionnaires, whether the data received under the Privacy Shield will be returned, deleted, or retained.

If the data will be retained, the organization must continue to apply the Privacy Principles to the data that was collected under the Privacy Shield even though it is no longer a participant. Moreover, the organization is required to appoint an individual to serve as an ongoing contact point for Privacy Shield-related questions. Note that in cases where the DOC has removed an organization from the Privacy Shield due to a "persistent failure" to comply with the Privacy Principles, that organization will be obliged to return or delete the personal data received under the Privacy Shield. In other cases of removal, the organization may retain such data if it annually affirms to the DOC its commitment to continue to apply the Privacy Principles to the previously collected data or otherwise provide adequate protection for the personal data by other authorized means such as EU standard contractual clauses.

ACCESS BY PUBLIC AUTHORITIES AND PRIVACY SHIELD OMBUDSMAN

In response to the perceived overreach of U.S. government surveillance, the Privacy Shield contains written assurances that government access to EU personal data for national security purposes is subject to clear conditions, limitations, and active oversight. In particular, the Privacy Shield incorporates Presidential Policy Directive 28 ("PPD-28"), which has a binding effect on U.S. intelligence agencies. PPD-28 requires collection and access to EU personal data by U.S. intelligence agencies to be "as tailored as feasible" rather than carried out on a "generalized basis." The U.S. has further agreed to limit bulk collection of personal data to what is strictly necessary and proportionate in order to achieve specific national security objectives.

EU citizens concerned about potential breaches of these binding commitments by the U.S. government can now refer their concerns to a newly appointed Privacy Shield Ombudsman, who will ensure that complaints have been properly investigated and will provide individuals with independent confirmation on whether U.S. laws have been complied with, or whether noncompliance has been remedied. EU citizens may even contact the Ombudsman about data transfers mechanisms other than the Privacy Shield, such as the standard contractual clauses or Binding Corporate Rules.

Access to the Ombudsman is just one of multiple redress possibilities now afforded to EU data subjects seeking to ensure their data privacy rights are protected in the event of U.S. government access. For example, the Judicial Redress Act[6]—signed into law just five days prior to the release of the terms of the Privacy Shield—allows EU citizens access to U.S. courts to bring certain civil actions against U.S. government agencies under the U.S. Privacy Act[7] for violations of their data protection rights. Moreover, EU data subjects can assert (limited) claims regarding electronic surveillance under the Foreign Intelligence Surveillance Act,[8] the Computer Fraud and Abuse Act,[9] and the Electronic Communications Privacy Act.[10] In addition, they can seek access to existing federal government records under the Freedom of Information Act,[11] subject to certain exceptions. All of these redress possibilities are intended to assure the EU Commission that U.S. law affords EU data subjects appropriate protection.

ANNUAL REVIEWS

Once the Privacy Shield is finalized, the European Commission and the U.S. will conduct joint annual reviews to monitor all aspects of the Privacy Shield and to ensure that access to data for law enforcement and national security purposes remains necessary and proportionate. Following each annual review, the Commission will submit a public report to the European Parliament and Council. Should the Commission determine

that there are clear indications of U.S. noncompliance with the Privacy Principles or otherwise conclude that the national security exception does not ensure adequate protection, the Commission will notify the DOC and request that appropriate measures be taken within a reasonable timeframe to remedy noncompliance. If the U.S. cannot satisfy the Commission's requests within the time allotted, the Commission will initiate steps to partially or completely suspend the adequacy decision underlying the Privacy Shield. Alternatively, the Commission may amend the adequacy decision to impose additional requirements on organizations before they can transfer European data under the Privacy Shield.

The entry into force of the GDPR should not affect the validity of the Privacy Shield nor require an extensive review of the Principles, which to a large extent reflect (or sometimes even go beyond) the rules in the GDPR. For example, the annual review foreseen in the Privacy Shield goes beyond what is the new GDPR, which requires such reviews only at least every four years.

NEXT STEPS FOR IMPLEMENTATION

The Privacy Shield does not yet have the force or effect of law in either the U.S. or the EU. In the EU, the full terms of the Privacy Shield will soon be subject to scrutiny by the Article 29 Working Party, which consists of representatives from all EU DPAs. The Working Party issued a statement on March 1, 2016, that it would publish its nonbinding opinion on the adequacy decision during its plenary meeting scheduled April 12–13, 2016. The adequacy decision would then be considered by the Article 31 Committee, a regulatory committee of EU Member State Representatives, which must approve the decision by a qualified majority before the Commission can finalize and adopt it.

Within 30 days of the Commission's final approval of the adequacy decision, the 128-page package containing the terms of the Privacy Shield will be published in the U.S. *Federal Register*, and soon after will become fully effective.

PRACTICAL IMPLICATIONS FOR COMPANIES

The implementation of the Privacy Shield is still months away. Until its enactment, companies considering transitioning to the Privacy Shield still need to identify alternative methods to legally transfer personal data across the Atlantic, including the EU's standard contractual clauses or Binding Corporate Rules. Companies face considerable risk by taking a wait-and-see approach with the Privacy Shield without replacing the now-defunct Safe Harbor as their preferred data transfer mechanism. DPAs in Europe have threatened to take action against companies continuing to use the Safe Harbor for data transfers to the U.S.[12]

Organizations previously certified under the Safe Harbor will need to carefully assess the new terms of the Privacy Shield as well as their own privacy policies in order to determine how—and whether—to make their own privacy practices compliant with the new regime requirement. Organizations previously relying on the Safe Harbor also need to consider whether it makes good business sense to invest in the Safe Harbor recertification process pending implementation of the Privacy Shield. Although the transition from the Safe Harbor to Privacy Shield remains unclear, companies maintaining their Safe Harbor certifications may find an easier transition to the Privacy Shield once the new framework becomes effective. Given the overlap in Privacy Principles and the resemblance between the two frameworks, companies recertifying that they meet the obligations of the less-onerous Safe Harbor may be able to more quickly pivot to the Privacy Shield as a basis to transfer EU data outside of Europe, provided they can meet the Privacy Shield's more stringent requirements. Companies recertifying compliance with the Safe Harbor, however, will remain subject to FTC enforcement notwithstanding that they cannot rely on the old framework to legally transfer EU personal data across borders.

Once the Privacy Shield takes effect, the Privacy Principles apply immediately upon self-certification, and self-certifying companies can reasonably expect heightened regulatory oversight. Organizations that certify to the Privacy Shield within the first two months following the framework's effective date will be given a grace period of up to nine months to "bring existing commercial relationships with third parties into conformity with the accountability for onward transfer principle." However, during this grace period, organizations that transfer data to third parties must still apply the Notice and Choice Privacy Principles and must further ensure that third-party recipients can provide the same level of protection guaranteed by the Privacy Principles.

LAWYER CONTACTS

For further information, please contact your principal Firm representative or one of the lawyers listed below. General email messages may be sent using our "Contact Us" form, which can be found at www.jonesday.com/contactus/.

Mauricio F. Paez
New York
+1.212.326.7889
mfpaez@jonesday.com

Paloma Bru
Madrid
+34.91.520.3985
pbru@jonesday.com

Undine von Diemar
Munich
+49.89.20.60.42.200
uvondiemar@jonesday.com

Olivier Haas
Paris
+33.1.56.59.38.84
ohaas@jonesday.com

Jonathon Little
London
+44.20.7039.5224
jrlittle@jonesday.com

Laurent De Muyter
Brussels
+32.2.645.15.13
ldemuyter@jonesday.com

Elizabeth A. Robertson
London
+44.20.7039.5204
erobertson@jonesday.com

Jennifer C. Everett, an associate in the Washington Office, and Michael La Marca, an associate in the New York Office, assisted in the preparation of this White Paper.

ENDNOTES

1 *See* Jones Day *Commentary*, "'EU-U.S. Privacy Shield' to Replace 'Safe Harbor'" (Feb. 2016).

2 *See* U.S. Department of Commence EU-U.S. Privacy Shield.

3 *See* EU Commission Press Release (Feb. 29, 2016).

4 *See* Jones Day *Commentary*, "EU–U.S. Data Protection Safe Harbor: Not Safe Anymore" (Oct. 2015).

5 Article 8 of the Data Protection Directive 95/46/EC defines "sensitive data" as personal data revealing racial origin, political opinions, or religious or philosophical beliefs; trade-union membership; and data concerning health or sex life. At some point, this is likely to be extended to genetic data, biometric data, and data about sexual orientation, as those are also qualified as sensitive data in Article 9 of the GDPR.

6 Pub. L. No. 114-126 (2016).

7 5 U.S.C. § 552a.

8 50 U.S.C. § 1801 *et seq.*

9 18 U.S.C. § 1030.

10 18 U.S.C. § 2510 *et seq.*

11 5 U.S.C. § 552.

12 *See* Statement of the Article 29 Working Party on the Consequences of the *Schrems* Judgment (Feb. 3, 2016).