EU-U.S. Privacy Shield Q & A

Jackson Lewis P.C.
www.jacksonlewis.com

jackson lewis
Preventive strategies.
Positive solutions.®

EU-U.S. Privacy Shield Q & A

Q-1. What is the EU-U.S. Privacy Shield?

Adopted on July 12, 2016, the EU-U.S. Privacy Shield (the "Privacy Shield") governs transfers of personal data from the EU to the U.S. for commercial purposes. The Privacy Shield replaces the former framework governing such transfers, the EU-U.S. Safe Harbor (the "Safe Harbor"), which was invalidated by the Court of Justice of the European Union's ("CJEU") October 6, 2015 decision, *Schrems v. Data Protection Commissioner*. The CJEU deemed the Safe Harbor scheme invalid on the basis that it failed to ensure that organizations transferring data from the EU to the U.S. would continue, post-transfer, to afford that data privacy protections essentially equivalent to those mandated under EU law.

Q-2. What impact does the Privacy Shield have on my organization here in the U.S.?

The European Commission has specified that existing U.S. law does not provide an adequate level of protection for personal data. As such, there are currently three primary mechanisms for transferring personal data of EU residents to the U.S. These mechanisms are binding corporate rules, standard contract clauses, and the Privacy Shield. Absent one of these three mechanisms, personal data of EU residents generally may not be transferred to the U.S., unless the 'unambiguous consent' of the data subject to transfer his or her personal data is obtained, and in some EU jurisdictions consent which is given as a condition of employment is not regarded as freely given.

Q-3. What new obligations does the Privacy Shield impose?

Organizations that opt to join the Privacy Shield are subject to the following six new requirements, among others: First, they must notify the public of their obligations under the Privacy Shield, such as by preparing a declaration of commitment to the Privacy Shield; by providing links on their websites to the Department of Commerce's Privacy Shield website; and by informing those whose data they hold of the protections afforded by the Privacy Shield. Second, participating organizations must provide free and accessible dispute resolution mechanisms. Third, they must cooperate with Department of Commerce ("DOC") inquiries and requests. Fourth, they are barred from maintaining irrelevant personal information, and must comply with the Privacy Shield's Data Integrity and Purpose Limitation Principle. Fifth, they are obligated to implement certain safeguards before transferring data to third parties. And sixth, in the event they are required by a Federal Trade Commission ("FTC") or court order to submit a compliance or assessment report, they must publish such report.

Q-4. Is my organization required to join the Privacy Shield?

No. Joining the Privacy Shield is voluntary. However, once an eligible organization publicly commits to compliance with the Privacy Shield, that commitment is enforceable under U.S. law. Compliance will be monitored by the DOC, and enforced by the FTC and Department of Transportation ("DOT"). As mentioned above, absent one of these three mechanisms, personal data of EU residents generally may

not be transferred to the U.S., unless the 'unambiguous consent' of the data subject to transfer his or her personal data is obtained.

Q-5. Is my organization eligible to join the Privacy Shield?

Any U.S. organization that is subject to the jurisdiction of the FTC or DOT is eligible to join the Privacy Shield. Practically speaking, most organizations with international operations should consider whether the Privacy Shield is the appropriate mechanism for them to transfer personal data of EU residents to the U.S. The FTC has jurisdiction over acts or practices in or affecting commerce by any "person, partnership, or corporation." It does **not** have jurisdiction over most depository institutions (*e.g.*, banks, federal credit unions, and savings & loan institutions), telecommunications and interstate transportation common carrier activities, air carriers, labor associations, most non-profit organizations, and most packer and stock yard activities. Additionally, its jurisdiction over insurance activities is limited. The DOT has exclusive jurisdiction over U.S. and foreign air carriers, and shared jurisdiction over ticket agents that market air transportation.

Q-6. Given that my organization is not required to join the Privacy Shield, why should it do so?

The European Commission has deemed the Privacy Shield an adequate mechanism to enable data transfers compliant with EU law. Absent self-certification under the Privacy Shield, to legally transfer personal data of EU residents to the U.S an organization generally must utilize either standard contract clauses or binding corporate rules.

Standard contractual clauses are often difficult to implement, may require approval by EU member states prior to transfer, and can involve difficult negotiations to gain agreement between data controllers and processors. The clauses cannot be modified, but the parties can rely on them to transfer data lawfully.

Implementing binding corporate rules offers some flexibility because internal rules governing protections for personal data can be tailored to address the needs of the organization. But, those rules must undergo a process of review and approval by regulators – a process that is complex, time-consuming and expensive. Few companies have completed this process.

Of course, organizations may secure the unambiguous and explicit consent of the data subject to transfer his or her data, but this is often not practical especially when working with data on large numbers of individuals, and in some EU jurisdictions the consent will not be recognized as valid if it is deemed required as a condition of employment. There also are limited statutory exceptions that might permit transfer in some cases, but the exceptions do not offer a comprehensive solution. Finally, organizations could anonymize the personal data for transfer. This can be a workable approach when an organization is engaged in audit and research functions, but not when it needs identifiable information, such as for human resources administration.

Joining (and, of course, thereafter complying with) the Privacy Shield therefore may give U.S. organizations an easier means to transfer personal data, while also providing some assurance that their data transfers from the EU will not expose them to liability under EU law. However, the Privacy Shield has

yet to be tested in court, and it will be some time before organizations gain a sense how the Privacy Shield and its Principles will be applied under the newly structured enforcement scheme.

Q-7. If my organization decides to join the Privacy Shield, when should it do so?

The DOC began accepting self-certifications to the Privacy Shield on August 1, 2016. As an added incentive to certify early, organizations that do so by October 1, 2016 will be given a nine-month grace period to "bring existing commercial relationships with third parties into conformity with the Accountability for Onward Transfer Principle." Even during the grace period, however, organizations will be subject to the Notice and Choice Principles, and must ensure that third-party recipients of transferred data provide protection equivalent to that guaranteed by the Privacy Shield Principles.

Q-8. If my organization decides to join the Privacy Shield, what does it need to do?

The DOC has issued guidance on joining the Privacy Shield, which contains a step-by-step Guide to Self-Certification. To expedite the self-certification process, organizations should compile certain information before logging on to complete the self-certification process.

The steps to self-certification are:

1. Confirm that your organization is eligible to participate, which it will be so long as its activities are subject to the jurisdiction of the FTC or DOT.
2. Commit to complying with the seven Principles governing the handling of personal data, and craft a privacy policy statement that specifies this agreement in compliance with the Privacy Shield.
3. Develop an independent recourse mechanism to investigate unresolved complaints (this mechanism must be free of cost to the complainant).
4. Implement procedures for verifying compliance with the Privacy Shield; these procedures can take the form of an internal self-assessment or external third-party assessment program.
5. Designate a contact, such as your Chief Privacy Officer, to receive questions, complaints, and access requests, and to handle other issues relating to the Privacy Shield.

The DOC has also provided a link to the self-certification forms.

Q-9. What are the Privacy Principles?

There are seven Privacy Principles governing the handling of personal data which an organization must commit to comply with in order to self-certify under the Privacy Shield. Those Principles, along with a brief summary of each, are:

- ***Notice:*** An organization must inform individuals about thirteen different data practices including the types of personal data collected and the purposes for which the personal data is collected.

- ***Choice:*** An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) 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. However, organizations must obtain affirmative express consent (opt in) for sensitive information (i.e., personal 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).

- ***Accountability for Onward Transfer:*** Organizations must enter into contracts with applicable third-party controllers that provide that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as exists under the Principles.

- ***Security:*** Organizations must take reasonable and appropriate measures to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction.

- ***Data Integrity and Purpose Limitation:*** Personal information must be limited to the information that is relevant for the purposes of processing. An organization may not process personal information in a way that is incompatible with the purposes for which it was initially collected or which the data subject subsequently authorizes. An organization must take reasonable steps to ensure that personal data is reliable for its intended use, and is accurate, complete, and correct.

- ***Access:*** Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, or has been processed in violation of the Principles.

- ***Recourse, Enforcement, and Liability:*** Effective privacy protection must include robust mechanisms for assuring compliance with the Principles, recourse for individuals who are affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed.

Q-10. How does the Privacy Shield address human resources data?

The seven Privacy Principles are accompanied by sixteen Supplemental Principles which provide additional requirements for certain types of data and address various data transfer issues. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the same. An organization that chooses to extend Privacy Shield benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies, and must conform to the Supplemental Principle on Self-Certification. In practice, if an organization does not extend the Privacy Shield benefits to human resources personal information, this data may only be legally transferred through either binding corporate rules, standard contract clauses or consent.

Q-11. What Supplemental Principle applies to human resources data?

Once self-certification extends Privacy Shield benefits to human resources personal information, an organization in the EU transferring personal information about its employees (past or present) that was collected in the context of the employment relationship, whether to a parent, affiliate, or unaffiliated service provider in the U.S. participating in the Privacy Shield, will enjoy the benefits of the Privacy Shield. In such cases, the collection of the information and its processing prior to transfer will have been subject to the national laws of the EU country where it was collected, and any conditions for or restrictions on its transfer according to those laws will have to be respected. The Supplemental Principle on Human Resources Data provides the following additional detail.

- ***Notice and Choice Principles***

  A U.S. organization that has received employee information from the EU under the Privacy Shield may disclose it to third parties or use it for different purposes only in accordance with the Notice and Choice Principles. For example, where an organization intends to use personal information collected through the employment relationship for non-employment related purposes, such as marketing communications, the U.S. organization must provide the affected individuals with the requisite choice before doing so, unless they have already authorized the use of the information for such purposes. Such use must not be incompatible with the purposes for which the personal information was initially collected or which the data subject subsequently authorizes . Moreover, such choices must not be used to restrict employment opportunities or to take any punitive action against such employees.

  Notably, certain generally applicable conditions for transfer from some EU Member States may preclude other uses of such information, even after transfer outside the EU, and such conditions will have to be respected.

  In addition, employers should make reasonable efforts to accommodate employee privacy preferences. This could include, for example, restricting access to the personal data, anonymizing certain data, or assigning codes or pseudonyms when the actual names are not required for the management purpose at hand.

  To the extent and for the period necessary to avoid prejudicing the ability of the organization in making promotions, appointments, or other similar employment decisions, an organization does not need to offer notice and choice.

- ***Access Principle***

  The Supplemental Principle on Access provides guidance on reasons which may justify denying or limiting access on request in the human resources context. Of course, employers in the European Union must comply with local regulations and ensure that European Union employees have access to such information as is required by law in their home countries, regardless of the location of data processing and storage. The Privacy Shield requires that an organization processing such data in the United States will cooperate in providing such access either directly or through the EU employer.

- ***Enforcement***

  In so far as personal information is used only in the context of the employment relationship, primary responsibility for the data vis-à-vis the employee remains with the organization in the EU. It follows that, where European employees make complaints about violations of their data protection rights and are not satisfied with the results of internal review, complaint, and appeal

procedures (or any applicable grievance procedures under a contract with a trade union), they should be directed to the state or national data protection or labor authority in the jurisdiction where the employees work. This includes cases where the alleged mishandling of their personal information is the responsibility of the U.S. organization that has received the information from the employer and thus involves an alleged breach of the Principles. This will be the most efficient way to address the often overlapping rights and obligations imposed by local labor law and labor agreements as well as data protection law.

A U.S. organization participating in the Privacy Shield that uses EU human resources data transferred from the European Union in the context of the employment relationship and that wishes such transfers to be covered by the Privacy Shield must therefore commit to cooperate in investigations by and to comply with the advice of competent EU authorities in such cases.

- ***Accountability for Onward Transfer Principle***
  For occasional employment-related operational needs of the Privacy Shield organization with respect to personal data transferred under the Privacy Shield, such as the booking of a flight, hotel room, or insurance coverage, transfers of personal data of a small number of employees can take place to controllers without application of the Access Principle or entering into a contract with the third-party controller, as otherwise required under the Accountability for Onward Transfer Principle, provided that the Privacy Shield organization has complied with the Notice and Choice Principles.

Q-12. Can an individual file a complaint if she believes an organization violated her privacy rights?

In a word, yes, and there is a robust framework for seeking recourse and enforcement. When organizations self-certify under the Privacy Shield, one of the Principles they must abide by is the Recourse, Enforcement and Liability Principle. Under this Principle, individual complaints and disputes must be investigated and resolved at no cost to the individual, and in a readily available and effective manner that can verify compliance.

Companies can establish an independent recourse mechanism either in the EU or in the U.S. For example, an organization might choose to cooperate with the EU DPAs, or implement independent Alternative Dispute Resolution ("ADR") or private-sector developed privacy programs that incorporate the Principles.

- ***Important –*** Note that when it comes to human resources data, companies must cooperate with the DPAs regardless of their choice above.

The bottom line is companies must remedy non-compliance. As discussed below, individuals can bring complaints directly to the organization, to an independent dispute resolution body designated by the organization, to national DPAs or to the FTC.

Q-13. What if the recourse mechanisms available to the individual do not work?

The Privacy Shield established the "Privacy Shield Panel" under which individuals can seek binding arbitration after certain available remedies have been exhausted.

Q-14. Is there a recommended path for seeking recourse?

In its implementing decision of July 12, 2016, the European Commission notes that individuals are free to pursue any or all available mechanisms, and are not obliged to choose one mechanism over another, or to follow a specific sequence. But, the Commission did recommend a "logical order" to follow:

1. Make direct contact with the U.S. self-certified organization.
2. Submit complaint to the independent dispute resolution body designated by the organization.
3. Complain to the national DPA. (Remember, in cases involving human resources data, the organization must cooperate with a DPA's investigation and resolution.)
4. Channel the complaint to the DOC through the national DPA.
5. Submit the complaint to the FTC.
6. Seek binding arbitration.

Of course, individuals may seek other legal or equitable remedies, such as contractual or tort remedies.

Q-15. What does the organization have to do if it receives a complaint from an individual concerning compliance with the Privacy Shield?

U.S. companies that have self-certified under the Privacy Shield and receive a complaint from an EU data subject should already have in place an effective redress mechanism to handle the complaint. It should follow that process. That process should include responding to the complaint within 45 days with an assessment of the merits of the complaint and how the organization will rectify the problem.

Q-16. If the individual complains to an independent dispute resolution body, must the organization comply with the decision of that resolution body?

As noted above, self-certifying companies must designate an independent dispute resolution body to investigate and resolve individual complaints free of charge to the individual. The companies' published privacy policies must include information about resolution body that can be used for this purpose. Under the Privacy Shield, the sanctions and remedies imposed by these bodies must be sufficiently rigorous to ensure compliance with the Principles, remediate the non-compliance, and publicize the findings.

If the independent dispute resolution body discovers that the organization did not comply with the body's ruling, it must notify the DOC and the FTC (or other applicable U.S. authority), or a competent court. Companies that are persistent offenders may find themselves removed from the list of approved Privacy Shield organizations by the DOC. The Department will not take this action, however, before providing 30 days' notice and an opportunity to respond.

Q-17. Does my organization have to maintain records of compliance with the Privacy Shield?

Yes. These records must be available upon request by a dispute resolution body or the FTC in the context of an investigation or a complaint about non-compliance.

Q-18. How must a U.S. organization handle a complaint that is made to a national Data Protection Authority?

As discussed above, for complaints concerning the processing of human resources data collected in the context of an employment relationship, and for companies that have voluntarily submitted to the oversight by DPAs, companies must respond to DPA inquiries, comply with the advice given by the DPA, including for remedial or compensatory measures, and provide the DPA with written confirmation that such actions have been taken. If the DPA panel is not the organization's designated dispute resolution body, the DPA may refer complaints either to the DOC or FTC.

For complaints handled by the DPA, both sides will have an opportunity to comment and to provide evidence. To ensure a harmonized and coherent approach, the DPAs' advice will be delivered through an informal panel of DPAs established at Union level. Decisions generally will be made within 60 days after receiving a complaint, and the organization will have approximately 25 days following delivery of the advice to comply, absent a satisfactory explanation for the delay. If the organization does not comply, the panel will give notice of its intention either (i) to submit the matter to the FTC (or other competent U.S. enforcement authority) which could lead to enforcement action by the FTC, or (ii) to conclude that the commitment to cooperate has been seriously breached, resulting in notice to the DOC and possibly removal from the Privacy Shield list.

Q-19. What role does the Department of Commerce play in resolving complaints?

The DOC will have a special arrangement with DPAs to receive and address complaints. A dedicated person at Commerce will track the complaint and follow up with companies to facilitate resolution. Thus, EU data subjects will be able to bring complaints of non-compliance directly to their national DPA and have them channeled to the DOC for a response within 90 days.

As noted above, the refusal to comply with a final determination by an independent dispute resolution or government body, including a DPA, will be regarded as a persistent failure to comply. When the DOC concludes that an organization has persistently failed to comply with the Principles, it will remove the organization from the Privacy Shield list.

Q-20. How will the FTC enforce the Privacy Shield?

Under the Privacy Shield, all self-certifying companies must be subject to the investigatory and enforcement powers of U.S. authorities, in particular the FTC. As with the DOC, the FTC will establish a point of contact to receive referrals of non-compliance from DPAs. These and other referrals from independent dispute resolution or self-regulatory bodies and the DOC will receive priority. The agency

also will accept complaints from individuals. While the agency generally has no power to conduct on-site inspections in the area of privacy protection, it can compel companies to produce documents and provide witness statements.

Currently, enforcement by the FTC concerning deceptive and unfair trade practices is carried out through administrative orders, and this also would apply concerning Privacy Shield violations. In the event an organization fails to comply with an order, the FTC may seek civil penalties and other remedies including injunctions in court. When a consent order is issued to an organization concerning the Privacy Shield, the organization will have certain self-reporting obligations and the FTC will add that organization to an online list of companies subject to FTC or court orders in Privacy Shield cases.

Q-21. When is binding arbitration available?

In general, if none of the available mechanisms resolve the complaint, binding arbitration is available as a recourse mechanism of "last resort." EU data subjects will be able to invoke arbitration when U.S. authorities (for instance, the FTC) have not satisfactorily resolved their complaints. The arbitration panel will consider the efforts and remedies provided by those authorities and mechanisms, but individuals can still seek arbitration if they consider the other remedies insufficient.

Q-22. How will arbitration work?

In the case of a dispute eligible for arbitration, the parties will select one or three arbitrators from a pool of at least 20 arbitrators designated by the DOC and the Commission. Standard rules will govern the arbitration proceedings, that will include the following features:

- EU data subjects can be assisted by their DPAs.
- EU data subjects can use telephone or video conference capabilities at no cost.
- Translation services will be made available at no cost, upon request.
- Eligible costs of the arbitration proceeding may be covered by a DOC fund, although each party must pay for their own attorneys.

The arbitration panel will have the authority to impose "individual-specific, nonmonetary equitable relief" to remedy non-compliance with the Principles. Individuals can enforce the arbitration decision in the U.S. courts under the Federal Arbitration Act.

Q-23. What should my organization do now?

As mentioned above, if your organization transfers personal data from the EU to the U.S., you should be determining which of the three available data transfer mechanisms you will use. The above Q&As provide insight into the Privacy Shield, which may be the easiest means for your organization to comply with the laws governing data transfers from the EU to the U.S. If you choose to join the Privacy Shield, we would recommend you review, with legal counsel, your current practices and policies to ensure compliance with the Privacy Shield's mandates.

For further information, please contact

Jason C. Gavejian
Jackson Lewis P.C.
200 Headquarters Plaza, 7th Floor
Morristown, NJ 07960 | 973.451.6346
Jason.Gavejian@jacksonlewis.com

John L. Sander
Jackson Lewis P.C.
666 Third Avenue, 29th Floor
New York, NY 10017 | 212.545.4050
John.Sander@jacksonlewis.com

Joseph J. Lazzarotti
Jackson Lewis P.C.
200 Headquarters Plaza, 7th Floor
Morristown, NJ 07960 | 973.451.6346
LazzarottiJ@jacksonlewis.com

Damon W. Silver
Jackson Lewis P.C.
666 Third Avenue, 29th Floor
New York, NY 10017 | 212.545.4063
Damon.Silver@jacksonlewis.com