

## ANNEX

### **Correction and Clarification of Statements in the European Parliament Resolution on the Adequacy of the EU-U.S. Privacy Shield**

---

**Paragraph 5:** The Parliament “highlights that during a sub-quorum period the PCLOB may not ... hire staff”.

#### Response

The FISA Amendments Reauthorization Act of 2017 provides that when the position of chair of the Privacy and Civil Liberties Oversight Board (PCLOB) is vacant, the other serving Board members may exercise the chair’s authority to appoint new PCLOB staff. Thus, during a sub-quorum period, the PCLOB may hire staff.

**Paragraph 7:** The Parliament “[r]eiterates its position that the Ombudsperson mechanism set up by the US Department of State is not sufficiently independent and is not endowed with sufficient effective powers to carry out its tasks and provide effective redress to EU citizens; stresses that the exact powers of the Ombudsperson mechanism need to be clarified, especially with regard to his/her powers vis-à-vis the intelligence community and the level of effective remedy of his/her decisions; regrets that the Ombudsperson can only request action by and information from US governmental bodies, and cannot order the authorities to cease and discontinue unlawful surveillance, or to permanently destroy information; points out that, while there is an acting Ombudsperson, to date the US administration has still not appointed a new permanent Ombudsman, which does not contribute to mutual trust; takes the view that in the absence of an appointed independent, experienced and sufficiently empowered Ombudsperson, the US assurances with regard to the provision of effective redress to EU citizens would be null and void”.

#### Response

First and most significantly, the Ombudsperson provisions of the Framework provide a mechanism pursuant to which EU authorities can submit requests on behalf of EU individuals regarding U.S. signals intelligence practices. The United States has complied fully with those provisions, creating a position that is independent of the intelligence community and reports directly to the Secretary of State. The Ombudsperson mechanism was established and implemented in 2016—and has remained ready for over two years to receive any such inquiries. Notably, no such inquiries have been received.

Second, by focusing solely in this context on the Ombudsperson mechanism, the Resolution overlooks the essential broader context that in making its adequacy decision, the European Commission considered “a number of avenues . . . available under U.S. law to EU data subjects if they have concerns whether their personal data have been

processed . . . by U.S. Intelligence Community Elements”, including the Ombudsperson mechanism. This context is important because the Ombudsperson mechanism was created to supplement other redress mechanisms also available to EU individuals.

Third, the Resolution’s statement that “the US administration has still not appointed a new permanent Ombudsman” and that there is an “absence of an appointed independent, experienced and sufficiently empowered Ombudsperson” suggests a misunderstanding of the U.S. system. Because the authorities of the Under Secretary of State for Economic Growth, Energy, and the Environment have been exclusively delegated to Ambassador Garber, she has served as the Privacy Shield Ombudsperson in accordance with the Framework. She has been fully empowered to carry out the functions and duties of the Privacy Shield Ombudsperson, with all the same authorities as her predecessor, including independence from the intelligence community and direct reporting to the U.S. Secretary of State.

That said, the Administration is extremely mindful of the expectation among EU officials for prompt selection of a politically appointed Under Secretary to serve as Ombudsperson, and the White House is working to announce a nominee in the coming months. In light of Ambassador Garber’s recent nomination to become U.S. Ambassador to the Republic of Cyprus, Secretary of State Pompeo has decided that the current Assistant Secretary of State for Economic and Business Affairs, Manisha Singh, will assume the duties of the Privacy Shield Ombudsperson until the new nominee for Under Secretary is confirmed by the U.S. Senate. As reflected in her biography (a copy of which is attached), Ms. Singh was herself confirmed unanimously by the Senate in 2017 and served previously as a Deputy Assistant Secretary of State in the Bureau of Economic, Energy and Business Affairs, and as Deputy Chief Counsel to the U.S. Senate Committee on Foreign Relations.

Until a new Under Secretary is confirmed, Ms. Singh will have the same authority to carry out the Ombudsperson function as Ambassador Garber has presently and as Catherine Novelli had previously. Neither of these officials is or was “permanent” and any person serving as Ombudsperson will be independent, experienced, and empowered in keeping with the terms of the Framework.

Finally, as to the Resolution’s concerns that the Ombudsman role may not be sufficiently clear, an unclassified version of the Ombudsperson implementation procedures has been made publicly available at <https://www.state.gov/e/privacysshield/ombud/> (*see Attachment 2*). This unclassified version is substantially identical to its classified counterpart, except in a very limited number of places where classified material was summarized in unclassified terms. The unclassified procedures make plain, including

through an illustrative example, that the Ombudsperson mechanism will—in working with the Intelligence Community and various oversight entities—ensure that any incidents of non-compliance identified in connection with a request are remedied.

**Paragraph 8:** The Parliament “deplores that until said confirmation four of the five FTC seats had remained vacant, considering that the FTC is the competent agency for enforcement of the Privacy Shield principles by US organizations”.

Response

The U.S. Federal Trade Commission (FTC) has had all five Commissioners in place since May 2018. Even prior to Senate confirmation of the full slate of Commissioners, the FTC remained fully functioning and effective in carrying out its enforcement responsibility under the Framework. For instance, the FTC brought enforcement actions against three Privacy Shield companies in September 2017.

**Paragraph 10:** The Parliament “considers that in order to ensure transparency and avoid false certification claims, the DoC should not tolerate US companies making public representations about their Privacy Shield certification before it has finalised the certification process and has included them on the Privacy Shield list”.

Response

This issue has now been addressed. Following the European Commission’s October 2017 report to the European Parliament and the European Council on the first annual review—which recommended that “[c]ompanies should not be able to publicly refer to their Private Shield certification before the certification is finalized by the DoC”—the U.S. Department of Commerce (DoC) instituted a change in program requirements (in close cooperation with the European Commission) to address the Commission’s concern. Since February 2018, companies certifying for the first time have been required to delay public representations regarding their Privacy Shield participation until their certification review is completed by DoC.

**Paragraph 10:** The Parliament “calls on the DoC to undertake proactively and on a regular basis *ex officio* compliance reviews to monitor the effective compliance of companies with the Privacy Shield rules and requirements”.

Response

DoC is already proactively monitoring participating organizations’ compliance with the Privacy Shield Principles. Early this year, DoC implemented a new process (in close cooperation with the European Commission) to conduct spot checks of randomly selected Privacy Shield participants in order to verify that: (1) the point(s) of contact responsible

for the handling of complaints, access requests, and other issues arising under Privacy Shield are available and responsive, (2) the organization’s privacy policy is freely and openly available for public viewing, (3) the organization’s privacy policy continues to comply with the self-certification requirements set forth in the Framework, and (4) the organization’s chosen independent recourse mechanism(s) is available to investigate and resolve complaints.

If there is credible evidence that a participating organization does not comply with its Privacy Shield commitments or if significant issues are identified during a compliance review, the organization receives a compliance questionnaire to which it must respond within 30 days. If the organization does not provide a timely and satisfactory response, DoC sends a warning letter requiring the organization to indicate within 30 days how it has addressed the identified issue(s). If after that 30-day period the issues have not been resolved, the organization is removed from the Privacy Shield List and placed on the Privacy Shield Inactive List. DoC makes referrals as appropriate to FTC for false claims enforcement.

These spot checks of randomly selected participants supplement DoC’s annual recertification process, to which all Privacy Shield participants are subject. During this mandatory annual review, DoC confirms that each recertifying participant has met all certification requirements.

**Paragraph 11:** The Parliament “recommends ... that the US authorities offer more concrete information on the Privacy Shield website in an accessible and easily understandable form to individuals regarding their rights and available recourse and remedies”.

#### Response

There are now numerous resources on the Privacy Shield website that explain clearly and concisely the rights and recourse mechanisms for EU individuals:

- *Information for EU and Swiss Individuals*—This new one-pager was designed to explain what Privacy Shield is and the rights and recourse mechanisms afforded to EU and Swiss individuals thereunder. See Attachment 3 and webpage: <https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t0000000QJdq>
- *My Rights Under Privacy Shield*—This Privacy Shield webpage explains to EU and Swiss individuals the rights afforded them under the Framework. See Attachment 4 and webpage: <https://www.privacyshield.gov/article?id=My-Rights-under-Privacy-Shield>

- *How to Submit a Complaint*—This Privacy Shield webpage explains to EU and Swiss individuals the recourse mechanisms provided under the Framework and how to submit a complaint (with relevant links to do so). See **Attachment 5** and webpage: <https://www.privacyshield.gov/article?id=How-to-Submit-a-Complaint>
- *How to Submit a Request Relating to U.S. National Security Access to Data*—This Privacy Shield webpage links to the State Department’s Ombudsperson webpage to explain how to submit a request relating to U.S. national security access to data transmitted from the EU or Switzerland to the United States. See **Attachment 6** and webpage: <https://www.privacyshield.gov/article?id=How-to-Submit-a-Request-Relating-to-U-S-National-Security-Access-to-Data>

**Paragraph 12:** The Parliament cites “recent revelations of misuse of personal data by companies certified under the Privacy Shield, such as Facebook and Cambridge Analytica” and “calls on the US authorities responsible for enforcing the Privacy Shield to act upon such revelations without delay in full compliance with the assurances and commitments given to uphold the current Privacy Shield arrangement and, if needed, to remove such companies from the Privacy Shield list” and “considers that the revelations clearly show that the Privacy Shield mechanism does not provide adequate protection of the right to data protection”.

Response

DoC has removed both Cambridge Analytica and its parent company, SCL Elections LTD, from the Privacy Shield List. In addition, the “Facebook and Cambridge Analytica” incident has been the subject of an ongoing investigation in the United States by the FTC since at least March 2018. See **Attachment 7** and webpage <https://www.ftc.gov/news-events/press-releases/2018/03/statement-acting-director-ftcs-bureau-consumer-protection>.

As provided for in the Framework, DoC will remove an organization from the Privacy Shield List if any privacy self-regulatory, independent dispute resolution, or government body determines that the company has persistently failed to comply with the Privacy Shield Principles.

Because a company’s self-certification to Privacy Shield and its public representation of Privacy Shield participation provide the legal basis for bringing an enforcement action against the company, suspension of Privacy Shield would only serve to reduce the privacy protections for EU individuals.

**Paragraph 18:** The Parliament “urges ... that the DoC work with the European Data Protection Authorities to provide more precise guidance as regards essential principles of the Privacy Shield

such as the Choice Principle, the Notice Principle, onward transfers, the controller-processor relationship and access”.

#### Response

In response to the recommendation of the European Commission after the first annual review, DoC has worked closely with EU data protection authorities (DPAs) to develop guidance on the Privacy Shield Principles, including the Accountability for Onward Transfer Principle and controller-processor relationships. That guidance is available at [www.privacyshield.gov/article?id=FAQs](http://www.privacyshield.gov/article?id=FAQs) (see Attachment 8).

**Paragraph 22:** The Resolution raises several concerns about the U.S. Government’s acquisition of data for national security purposes under Section 702 of the Foreign Intelligence Surveillance Act (FISA Section 702), and requests clarification about selection of targets and the tasking of selectors thereunder.

#### Response

This paragraph is internally inconsistent, calling for evidence that FISA Section 702 does not involve bulk collection and then noting the explanation in the European Commission Staff Working Document that Section 702 “does not allow for collection in bulk”. The fact that Section 702 requires targeted collection and prohibits collection in bulk is also confirmed by the PCLOB’s publicly available 2014 report on FISA Section 702.

In addition, the PCLOB report addresses other concerns raised in paragraph 22 of the Resolution. Regarding selection of Section 702 targets, the PCLOB explains (at pages 20-24) that targets must be non-U.S. persons located outside the United States expected to communicate the type of foreign intelligence approved in a specific certification approved by the FISA Court. Regarding tasking of selectors, the PCLOB explains (at pages 32-37) that, for both PRISM and Upstream collection, the government gives selectors (*e.g.*, email addresses or telephone numbers) to a U.S.-based electronic communications service provider that has been served a directive pursuant to a FISA Court-approved certification, so that the provider is compelled to give the government communications sent to or from the selector.

The PCLOB report also discussed providers giving the government communications “about” a selector in Upstream, referring to communications not to or from a selector, but containing the selector in the text of the communication. Since the PCLOB published its report, the U.S. government has ended “about” collection.

Paragraph 22 asks for more information about use of selectors in Upstream data acquisition. As explained on pages 36-37 of the PCLOB report, which discusses the



process of upstream collection, selectors tasked from upstream internet transaction collection must be specific selectors (such as an email address) and may not be key words or the names of the targeted individuals. Only after being screened against the selectors are communications ingested into government databases.

More importantly, the U.S. system of privacy protections and safeguards against abuses of FISA Section 702 authorities are the same kinds of protections and safeguards required by the European Court of Human Rights (“ECtHR”) when it reviews the national security surveillance regimes of EU Member States—namely: (1) clear and accessible laws restricting the scope of permissible surveillance, (2) authorization procedures for surveillance, (3) limitations on the duration of surveillance, (4) procedures restricting the querying, retention, and dissemination of the information acquired, (5) independent oversight mechanisms, (6) other non-judicial remedies such as the kind offered by the Privacy Shield Ombudsperson mechanism, and (7) judicial remedies providing individuals access to information about them or judicial review of government claims of secrecy, and redress for unlawful intelligence activities by the government.

**Paragraph 25:** The Resolution raises a concern about obstacles faced by non-U.S. citizens to obtaining civil redress in U.S. courts due to the requirements of U.S. “standing” doctrine: “Highlight[ing] the persisting obstacles concerning redress for non-US citizens subject to a surveillance measure based on section 702 FISA or Executive Order 12333 due to the procedural requirements of ‘standing’ as currently interpreted by the US courts ...”

#### Response

The requirements of the U.S. constitutional doctrine of standing apply to all persons bringing claims in U.S. courts—whether they are non-U.S. citizens, U.S. citizens, or foreign or domestic corporations.

Under U.S. standing doctrine, a court has jurisdiction provided that the plaintiff has personally suffered an injury that is traceable to the conduct challenged and can be redressed by a court decision. Standing is a requirement of the U.S. Constitution that applies to all claims in U.S. courts, regardless of the subject matter or whether the government is a party to the litigation. The U.S. Supreme Court has held that this requirement serves an “overriding and time-honored concern about keeping the Judiciary’s power within its constitutional sphere”, to “prevent the judicial process from being used to usurp the powers of the political branches.” *Hollingsworth v. Perry*, 570 U.S. 693, 704 (2013). The requirement cannot be waived by the government.

Claimants challenging surveillance programs in U.S. courts have succeeded in some cases in establishing standing by showing the government has collected information

about them. *See, e.g., ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (claimants “surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them”). In certain proceedings, however, such as Freedom of Information Act suits for documents withheld by an agency or requests submitted to the Privacy Shield Ombudsperson, claimants need not establish collection of information about themselves.

We understand that similar doctrines of standing are common among EU Member States. Admissibility restrictions on claims brought in civil litigation are a fundamental feature of any legal system based on separation of powers and with an independent judiciary. In fact, a European Parliament report that found that the courts of nine EU Member States require claimants to establish “a direct personal interest in the action” for their claims to be admissible. *See* European Parliament, Directorate-General for Internal Policies, *Standing up for your right(s) in Europe: A Comparative Study on Legal Standing (Locus Standi) before the EU and Member States’ Courts* at 13 (2012).

The EU Fundamental Rights Agency has also confirmed that certain EU Member State courts, like U.S. courts, dismiss individuals’ claims alleging unlawful intelligence surveillance where the claimants cannot show their data has been collected by the government. *See* EU Fundamental Rights Agency, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU—Mapping Member States Legal Frameworks* at 67 (2015).

**Paragraph 26:** The Resolution raises a concern about the impact of Executive Order 13678 on data protections for EU citizens. Specifically, the Parliament “[e]xpresses its concern about the consequences of Executive Order 13768 on ‘Enhancing Public Safety in the Interior of the United States’ for judicial and administrative remedies available to individuals in the US, because the protections of the Privacy Act no longer apply to non-US citizens; takes note of the Commission’s position that the adequacy assessment does not rely on the protections of the Privacy Act and that therefore this Executive Order does not affect the Privacy Shield; considers that Executive Order 13768 does however indicate the intention of the US executive to reverse the data protection guarantees previously granted to EU citizens and to override the commitments made towards the EU during the Obama Presidency”.

#### Response

Executive Order 13768 is not relevant to Privacy Shield. As acknowledged in Paragraph 26 of the Resolution, the European Commission itself confirmed that the Executive Order does not affect Privacy Shield because Privacy Shield protections are not dependent on the Privacy Act, which is the focus of Section 14 of the Executive Order.



The statement later in Paragraph 26—that “Executive Order 13768 however indicates the intention of the U.S. executive to reverse the data protection guarantees previously granted to EU citizens and to override the commitments made towards the EU during the Obama Presidency”—is unfounded. No “data protection guarantees previously granted to EU citizens” are impacted by Executive Order 13768, because the Executive Order applies only “to the extent consistent with applicable law”. Thus, the Executive Order does not impact any legal rights that EU citizens have under the Judicial Redress Act, the Freedom of Information Act, or any other statute or regulation. Moreover, U.S. Secretary of Commerce Wilbur Ross and the White House have both confirmed publicly that the United States commitment to the Privacy Shield could not be stronger. See [Attachment 9](#) and webpage <https://www.whitehouse.gov/briefings-statements/statement-press-secretary-eu-u-s-privacy-shield/>.

**Paragraph 27:** The Resolution raises concerns about the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), alleging that it expands law enforcement access to data and could conflict with EU data protection laws. The Parliament “[e]xpresses its strong concerns regarding the recent adoption of the ... CLOUD Act (H.R. 4943), which expands the abilities of American and foreign law enforcement to target and access people’s data across international borders without making use of the mutual legal assistance (MLAT) instruments, which provide for appropriate safeguards and respect the judicial competences of the countries where the information is located; highlights that the CLOUD Act could have serious implications for the EU as it is far-reaching and creates a potential conflict with the EU data protection laws”.

#### Response

The CLOUD Act involves access to data for law enforcement purposes and does not expand the powers of criminal law enforcement authorities. It does not conflict with the Privacy Shield Framework, which provides a legal basis under EU law for transfers of personal data from the EU to participating U.S. organizations. The Privacy Shield Framework is unrelated to, and unaffected by, the CLOUD Act.

The CLOUD Act merely clarified that under the Stored Communications Act, which is one U.S. statutory basis for law enforcement investigations, a provider subject to the jurisdiction of the United States who receives a search warrant is obligated to produce responsive data within its control, no matter where the provider has chosen to store it. A warrant under the CLOUD Act must satisfy the same constitutional and statutory protections applicable to other warrants, including probable cause and particularity, based on a sworn affidavit, to the satisfaction of an independent judge before the government may obtain the requested information.

The Cloud Act does not impose any new legal requirements. It merely reaffirms the way the Stored Communications Act has always been applied by the courts in the United States. It also mirrors the obligation of a person subject to the jurisdiction of the United States to produce paper records and physical evidence pursuant to a U.S. subpoena, no matter where the records are located.

Only a single 2016 court ruling had adopted a narrower interpretation of the statute; every other U.S. court to issue a written opinion on the application of the Stored Communications Act has disagreed with that narrow reading. That 2016 ruling was pending before the U.S. Supreme Court when the CLOUD Act was enacted. Because of the enactment of the CLOUD Act, however, the 2016 ruling was vacated and dismissed.

This approach clarified by the CLOUD Act is the same approach taken under the laws of many other rights-respecting countries, including in Europe, in authorizing law enforcement investigators to obtain a warrant to compel the disclosure of evidence stored outside their nation's borders. The ability to compel a person within a country's territory to produce data within their control is also required by Article 18 of the Budapest Convention.

With respect to strengthening the use of requests pursuant to a Mutual Legal Assistance Treaty (MLAT), the U.S. Department of Justice (DOJ) has significantly expanded the resources dedicated to sending and responding to requests for assistance from all countries, including from the EU. Among other steps, DOJ substantially expanded the number of attorneys and paralegals focused on the MLAT process, and even created a unit dedicated to handling in-bound requests for electronic data.

In an increasingly digitized world, the MLAT process is a woefully insufficient mechanism to meet the needs of law enforcement to access electronic evidence held by providers that operate in their territory but are based in other countries. Because such providers may have conflicting legal obligations regarding disclosure of data to law enforcement, the CLOUD Act set up a mechanism to enter into bilateral agreements to reduce conflicts associated with obtaining electronic evidence held by such providers.

The European Commission is also actively seeking to address this same issue and proposed its own e-evidence Regulation and Directive to enable EU law enforcement authorities to obtain content data and metadata (*i.e.*, e-evidence) directly from providers—including electronic communications service providers, cloud providers, social networks, online marketplaces, hosting service providers, and providers of internet infrastructure such as IP address and domain name registries—based across national borders outside the EU.

**Paragraph 29:** The Resolution asserts that “US authorities have failed to proactively fulfil their commitment to provide the Commission with timely and comprehensive information about any developments that could be of relevance for the Privacy Shield”.

Response

U.S. authorities engage regularly and actively with the European Commission regarding Privacy Shield, coordinating on program implementation, discussing developments of relevance to the Framework, and addressing questions as they arise. Regarding the specific developments cited in paragraph 29, the U.S. Government provided information to the European Commission about Executive Order 13768, and the Privacy Rules for ISPs were discussed at the first annual review of the Framework in September 2017. U.S. Government officials have also briefed the European Commission about other matters, such as the amendments to U.S. law relevant to Privacy Shield in the FISA Amendments Reauthorization Act of 2017.

**Paragraph 30:** The Resolution complains of a lack of information about judicial redress rights for EU individuals with respect to potential use of their personal data by U.S. authorities for law enforcement and public interest purposes.

Response

In its adequacy determination of July 2016, The European Commission discusses potential access to and use of personal data by U.S. public authorities for law enforcement and public interest purposes at recitals (125) to (135) (*see Attachment 10*), including rights of judicial redress. The Commission concluded that U.S. law ensures effective legal protection against interference for law enforcement or other public interest purposes with the fundamental rights of persons whose personal data are transferred from the EU to the United States under the Privacy Shield Framework.

## Attachment 1

### **Manisha Singh**

*Assistant Secretary of State, Bureau of Economic and Business Affairs*



Manisha Singh was unanimously confirmed by the Senate and sworn in as Assistant Secretary of State on November 22, 2017. She leads a team of over 200 employees in the Bureau of Economic and Business Affairs which also serves as the home bureau for economic officers posted in embassies around the world. She is the first woman appointed to the role and is responsible for advancing American prosperity, entrepreneurship and innovation worldwide.

Ms. Singh served previously as the Deputy Assistant Secretary in the Bureau of Economic, Energy and Business Affairs. In that role, she was responsible for developing and promoting international trade policy. She also worked as a senior aide to members of Congress and as Deputy Chief Counsel to the U.S. Senate Committee on Foreign Relations, where she managed international economic policy.

Ms. Singh's private sector experience includes practicing law at multinational law firms and working in-house at an investment bank. She was also the Senior Fellow for International Economic Affairs at the American Foreign Policy Council as well as a term member at the Council on Foreign Relations.

Ms. Singh completed a Master of Laws (LLM) in International Legal Studies, with concentration in international trade, at the American University Washington College of Law. While completing this degree, she worked in the Office of General Counsel at the United States International Trade Commission.

Her educational background also includes earning a Juris Doctor (JD) from the University of Florida College of Law and completing a Certificate at the University of Leiden in The Netherlands. She earned a Bachelor of Arts (BA) with honors at the University of Miami at the age of 19. She is admitted to practice law in Florida, the District of Columbia and Pennsylvania. She speaks fluent Hindi and conversational Spanish.

## Attachment 2

### **Privacy Shield Ombudsperson Mechanism Unclassified Implementation Procedure**

(U) **PURPOSE:** The Privacy Shield Ombudsperson Mechanism Implementation Procedure (Procedure) governs the implementation of commitments undertaken by the Department of State (Department) pursuant to EU-U.S. Privacy Shield Ombudsperson Mechanism Regarding Signals Intelligence (Ombudsperson Mechanism) under the EUU.S. Privacy Shield Framework (Framework) and other comparable arrangements extending the Privacy Shield Ombudsperson Mechanism. It assigns responsibilities for the review of allegations that the U.S. Intelligence Community has engaged in signals intelligence activities that do not comply with applicable restrictions affecting the personal privacy of unconsenting persons covered under the Ombudsperson Mechanism. The Department of State takes seriously allegations that U.S. signals intelligence activities have been conducted in a manner that fails to comply with applicable privacy protections and other restrictions. This Procedure is implemented consistent with applicable U.S. laws, policies, and procedures.

(U) **ROLES AND RESPONSIBILITIES:**

(U) **The Privacy Shield Ombudsperson (Ombudsperson)** oversees implementation of this Procedure and performs certain other specified functions contained herein. The Framework directs the Department's Senior Coordinator for International Information Technology Diplomacy under Presidential Policy Directive 28: Signals Intelligence to serve as the Ombudsperson. The Under Secretary of State for Economic Growth, Energy, and the Environment (E) has been designated as the Senior Coordinator for International Information Technology Diplomacy. The Under Secretary reports directly to the Secretary of State. To carry out the Ombudsperson duties, the Under Secretary will work closely with other U.S. government officials and agencies, including appropriate independent oversight bodies, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies.

(U) **The Office of International Communications and Information Policy (EB/CIP)** performs chief implementation functions under this Procedure. EB/CIP will update the Bureau of European and Eurasian Affairs (EUR) on an at least monthly basis as to the number of requests and responses under the Mechanism.

(U) **The Bureau of Intelligence and Research (INR)** advises the Ombudsperson and EB/CIP concerning intelligence issues and coordinates as appropriate with Intelligence Community (IC) partners. (U) The Office of the Legal Adviser (L) provides legal advice and coordinates as appropriate with IC partners.

(U) **The Bureau of Public Affairs (PA)** administers the public-facing Ombudsperson website.

(U) **The Bureau of Information Resource Management (IRM)** designs and provides technical support to the password-controlled Privacy Shield Ombudsperson Request Website.

(U) PROCESS:

(U) The EU Individual Complaint Handling Body (CHB)<sup>1</sup> submits perfected requests, consistent with paragraph 3.b. of the Ombudsperson Mechanism section of the Framework, for review to the Ombudsperson via a web portal that feeds into the Department's SharePoint site. The perfected request for review consists of the EU individual's request and a form completed by the CHB during its assessment.

(U) Initial Vetting and Disposition:

(U) Upon receiving each request for review, EB/CIP:

- ensures that the SharePoint site has automatically generated an individual tracking number and sent a confirmation of receipt to the CHB (these functions should occur automatically); and
- reviews the request to confirm it contains all required elements under paragraph 3.b. of the Ombudsperson Mechanism, which are:
  - the request contains information that –
    - forms the basis of the request;
      - Note: such information must contain at least one unique identifier associated with the type(s) of communications that are the subject of the request (examples are a telephone number or email address); a request that does not contain a unique identifier is deficient
    - states the nature of information or relief sought;
    - identifies the U.S. government entities believed to be involved, if any; and
    - cites any other measures the individual has taken to obtain the information/relief requested and the response received, if any; and
  - the CHB has –
    - confirmed verification of the requestor's identity;
    - concluded that the request concerns data reasonably believed to have been transferred under a covered mechanism; and

---

<sup>1</sup> References to the CHB throughout are also intended to apply to similar bodies under comparable arrangements.



- determined that the request is not frivolous, vexatious, or made in bad faith.

(U) In the course of this review, EB/CIP makes one of three determinations, in consultation with the Ombudsperson, INR, L, and other offices as necessary:

- the request does appropriately seek review under the Ombudsperson Mechanism but is deficient in one or more aspects (e.g., lack of identifier);
- the request does not appropriately seek review under the Ombudsperson Mechanism and is better understood as a request for records under the Freedom of Information Act (FOIA); or
- the request is sufficient

(U) *Deficient Requests:* Requests that either do not contain a unique identifier or state the nature of information or relief sought, or that may not have been sufficiently reviewed by the CHB will be returned to the CHB, via the SharePoint portal, along with a letter signed by the Director of EB/CIP/BA, or his or her designee, that details the deficiencies to be remedied. This letter should refer to the request by its individual tracking number.

(U) *FOIA Requests:* Requests that exclusively seek the production of or access to documents or other U.S. agency records may be best construed as FOIA requests. Uncertainty as to the nature of the request may require consultation with L and will be resolved in favor of processing the request under the Ombudsperson Mechanism. FOIA requests will be returned to the CHB, via the SharePoint portal, along with a letter signed by the Director of EB/CIP/BA, or his or her designee, that explains the Department's assessment and provides information on how to submit FOIA requests.

(U) *Sufficient Requests:* Requests that contain the required information listed above are deemed sufficient. If a sufficient request also seeks the production of documents, it should be processed for review under the Ombudsperson Mechanism and the final response letter should both contain the Ombudsperson's substantive response and provide information on how to submit a FOIA request. Sufficient requests are further processed through interagency processes contemplated in Section 2 of the Ombudsperson Mechanism in accordance with applicable classified procedures.

(U) This initial vetting process is to be completed within fifteen (15) days of receiving the request unless the volume of incoming requests requires additional resources. Should this occur, EB/CIP shall inform the Ombudsperson and seek her or his guidance, in consultation with INR and L as appropriate.

(U) Coordination:

(U) *Status Updates:* Should the CHB request information concerning the status of an individual request, EB/CIP will coordinate the preparation of a brief response confirming that the

request is in process. Any such status updates will refer to the request by its individual tracking number and are to be recorded in a mailbox associated with the SharePoint system.

(U) *Compliance Incidents:* In the event that further processing pursuant to applicable classified procedures reveals a compliance incident, pertinent implementation processes pursuant to such procedures shall be followed to ensure the compliance incident is remedied.

- (U) Because the further processing discussed in the preceding paragraph might contain or indirectly reveal information that risks disclosure of sources and methods, it is critically important that any information associated with such processing be classified and treated as extremely sensitive.
- (U) If, after these procedures have been followed, the Ombudsperson assesses that further review is required, the Ombudsperson will pursue such review as contemplated in Section 2 of the Ombudsperson Mechanism, including its provision that when the request relates to the compatibility of surveillance with U.S. law, the Privacy Shield Ombudsperson will be able to cooperate with one of the independent oversight bodies with investigatory powers, in accordance with applicable classified procedures.

(U) *Example of Coordination to Review Sufficient Requests:* Sufficient requests are processed in accordance with applicable classified procedures. The following example of how coordination might occur is drawn from unclassified descriptions of applicable existing oversight processes and is included for illustrative purposes:

- Once a sufficient request received by the Ombudsperson is determined to pertain to a particular Intelligence Community agency or element, the request will be reviewed by that agency or element's Civil Liberties and Privacy Office and forwarded to relevant officials, such as compliance officials, to conduct further reviews and to report their findings. The Office of the Intelligence Community Inspector General will be informed of all such requests and can conduct an independent review of any allegation of improper signals intelligence activity at any time.
- If a review finds a violation of law, executive order, or presidential directive, then appropriate measures would be taken to remedy the violation, including any required purge of data or recall of intelligence reporting. In addition, the incident would be reported through established incident reporting channels. Depending on the type of incident, this could include reporting to the Office of the Director of National Intelligence, the Department of Defense, the President's Intelligence Oversight Board, the Privacy and Civil Liberties' Oversight Board, the specific Inspector General for the agency or element in question, and intelligence oversight committees in Congress. If the incident involves a violation of any authority or approval granted by the Foreign Intelligence Surveillance Court, including for example, a violation of FISA Section 702 targeting procedures or minimization procedures, the violation would be reported to the Court.

- If the Ombudsperson determined an issue arose under the jurisdiction of another oversight authority, such as another Inspector General or the Privacy and Civil Liberties Oversight Board, the Ombudsperson can further refer the matter to them.
- The Ombudsperson would engage this oversight structure to ensure the incident is remedied.

(U) Responding to Sufficient Requests:

(U) Where there is no compliance incident detected, or where any compliance incident discovered has been remedied, EB/CIP prepares a letter for the Ombudsperson's signature certifying that U.S. laws, statutes, executive orders, presidential directives, and agency policies/regulations described in the ODNI letters incorporated into the Framework have been complied with, or, in the event of non-compliance, that such non-compliance has been remedied. Once signed, EB/CIP transmits the response to the CHB via the SharePoint portal.

(U) Improper Influence:

(U) Should the Ombudsperson have reason to believe an entity or individual inside or outside the Department is attempting to assert improper influence over the Ombudsperson Mechanism generally or over a specific request, the Ombudsperson will immediately report any and all such improper conduct to the Secretary, who will take any actions he deems appropriate to ensure that the Ombudsperson carries out its function objectively and free from improper influence that is liable to have an effect on the response to be provided. The Ombudsperson can also refer any such attempts to the appropriate Inspector General. Suspected criminal activity is reportable to Diplomatic Security and/or the Department of Justice, consistent with applicable Department guidance.

(U) Closing a File:

(U) Before marking a request as completed, EB/CIP ensures that all pertinent documentation is recorded in the appropriate system.

## Attachment 3



# The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks Information for EU and Swiss Individuals

### **What is the Privacy Shield?**

The EU-U.S. and Swiss-U.S. Privacy Shield Frameworks were designed by the U.S. Department of Commerce, and the European Commission and Swiss Administration, respectively, to provide a mechanism through which U.S.-based companies can comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

### **How Can I Learn Which Organizations Participate in Privacy Shield?**

The Privacy Shield team at ITA maintains the authoritative list of Privacy Shield participants at [www.privacyshield.gov/list](http://www.privacyshield.gov/list). To determine whether an organization is a participant, search alphabetically or type in the organization's name in the search bar. Click on the name of a participant to access the organization's Privacy Shield record. Participants' published privacy policies must also include information regarding their Privacy Shield participation, a link to the Privacy Shield website, contact information, and their selected independent recourse mechanism.



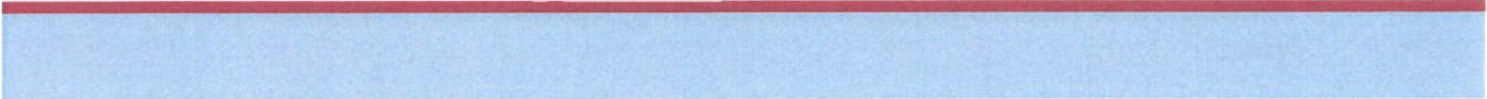
### **What Are My Rights Under Privacy Shield?**

A participating organization must provide you:

- Information on the types of personal data collected, the purposes of collection and use, and the type or identify of third parties to which your personal data is disclosed
- Choices for limiting use and disclosure of your personal data
- Access to your personal data
- Notification of the organization's liability if it transfers your personal data and the requirement to disclose your personal data in response to lawful requests by public authorities
- Reasonable and appropriate security for your personal data

### **How Do I Submit a Complaint Under Privacy Shield?**

- *Contact the organization*: This should be your first step. Contact information is accessible under "Questions or Complaints?" in the organization's Privacy Shield record and in its published privacy policy. The organization must respond within 45 days.
- *Contact the free independent recourse mechanism (IRM)*: IRM contact information is also accessible in the Privacy Shield record and published privacy policy.

- **Contact your data protection authority (DPA):** You can always submit a complaint directly to your local EU DPA or the Swiss Federal Data Protection and Information Commissioner.
  - **Invoke binding arbitration:** If your complaint is not resolved by the mechanisms described above, you may have the ability to invoke binding arbitration.
  - **Contact the U.S. enforcement authority:** Each organization's Privacy Shield record indicates the relevant U.S. enforcement authority. In most instances, it is the U.S. Federal Trade Commission (FTC). See: [ftccomplaintassistant.gov](https://ftccomplaintassistant.gov)
- 

## Attachment 4

# My Rights under Privacy Shield

**Among other requirements, a participating organization must provide you:**

- Information on the types of personal data collected
- Information on the purposes of collection and use
- Information on the type or identity of third parties to which your personal data is disclosed
- Choices for limiting use and disclosure of your personal data
- Access to your personal data
- Notification of the organization's liability if it transfers your personal data
- Notification of the requirement to disclose your personal data in response to lawful requests by public authorities
- Reasonable and appropriate security for your personal data
- A response to your complaint within 45 days
- Cost-free independent dispute resolution to address your data protection concerns
- The ability to invoke binding arbitration to address any complaint that the organization has violated its obligations under the Principles to you and that has not been resolved by other means

**As we work with our partners in the European Union and Switzerland to implement the Privacy Shield, we will provide additional information to help EU and Swiss individuals understand and exercise their rights.**



## Attachment 5

# How to Submit a Complaint

## Contact the organization

- Many of your questions or concerns can be addressed most quickly by contacting the Privacy Shield organization directly. This should be your first step. You can do this by typing the organization's name into the search bar within the [Privacy Shield List](#), clicking on the organization's name, and then clicking "Questions or Complaints?" The organization must respond to you within 45 days, though most issues can be addressed more quickly.

## Contact the free independent recourse mechanism

- If your question or concern is not addressed by contacting the organization directly, you can submit a complaint to the Privacy Shield organization's independent recourse mechanism. The contact information for the independent recourse mechanism is in the Privacy Shield organization's privacy policy and can also be found by clicking on the same "Questions or Complaints?" tab mentioned above.

## Contact your data protection authority (DPA)

- You can always submit a complaint directly to your [local DPA](#) or the Swiss Federal Data Protection and Information Commissioner. Your DPA or the Swiss Commissioner may refer your complaint directly to the Department of Commerce on your behalf. If referred to the Department of Commerce, the Privacy Shield Team will then work with the organization to seek to resolve your concern.

## Invoke binding arbitration

- If your complaint is not resolved after following the recourse mechanisms described above, you may have the ability to invoke binding arbitration. Additional information is available [here](#).

## Contact the U.S. enforcement authority

- Each organization's Privacy Shield record indicates the relevant U.S. enforcement authority. In most instances, the relevant U.S. enforcement authority is the Federal Trade Commission (FTC). To submit a complaint to the FTC, click [here](#). The FTC uses complaints in its database, which is accessible by many other law enforcement agencies, to identify trends, determine enforcement priorities, and identify potential investigative targets. Please note that the FTC does not resolve or mediate individual complaints, so you are encouraged to use the other complaint resolution mechanisms noted above as well. The only Privacy Shield participants not regulated by the FTC are U.S. and foreign air carriers, in which cases complaints can be submitted to the U.S. Department of Transportation (DOT) [here](#). The FTC and DOT share jurisdiction over ticket agents that market air transportation.

## Attachment 6

# Privacy Shield Ombudsperson



The Under Secretary of State for Economic Growth, Energy, and the Environment serves as the Privacy Shield Ombudsperson, a position dedicated to facilitating the processing of requests from EU and Swiss individuals relating to national security access to data transmitted from the European Union or Switzerland to the United States. Applicable data transfers include those conducted pursuant to the [EU-U.S. Privacy Shield Framework](#), [U.S.-Swiss Privacy Shield Framework](#), standard contractual clauses (SCCs), binding corporate rules (BCRs), and “Derogations” or “Possible Future Derogations.” This role builds on the Under Secretary’s position under [Presidential Policy Directive 28](#) as the Senior Coordinator for International Information Technology Diplomacy, which includes serving as a point of contact for foreign governments to raise concerns regarding signals intelligence activities conducted by the United States.

The Under Secretary reports directly to the Secretary of State and is independent from the Intelligence Community. To carry out the Ombudsperson duties, the Under Secretary works closely with other United States Government officials, including independent oversight bodies such as inspectors general, as appropriate, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies, including the [Ombudsperson Mechanism Implementation Procedures](#).

Acting Assistant Secretary [Judith G. Garber](#) was delegated the authorities of the Under Secretary for Economic Growth, Energy and the Environment (which includes those of the Ombudsperson under the EU-U.S. and Swiss-U.S. Privacy Shield Frameworks), pursuant to Delegation of Authority No. 415, dated January 18, 2017.

### **Request Submission Process:**

#### *STEP 1: Individual Submits a Request*

- EU individuals submit a request via the EU designated individual complaint handling body through their local [Data Protection Authority \(DPA\)](#).
- Swiss individuals submit a request via the [Federal Data Protection and Information Commissioner \(FDPIC\)](#)

### *STEP 2: Review by Relevant Authority*

The EU or Swiss authority confirms the identity of the requestor and verifies that the request fulfills the following criteria established in the Ombudsperson Mechanism:

- the request is complete (see "Information to Include" section below);
- the requestor is acting on his/her own behalf, and not as a representative of a governmental or intergovernmental organization;
- the request pertains to data reasonably believed to have been transferred under the Privacy Shield; and
- the request is not frivolous, vexatious, or made in bad faith.

### *STEP 3: Transfer to Ombudsperson*

If the EU or Swiss authority determines that the request meets the criteria, it then transmits the request to the Ombudsperson.

### *STEP 4: Response*

The Ombudsperson will transmit the review findings through the EU individual complaint handling body or the FDPIC.

### **Information to Include:**

Section 3.b of the [Ombudsperson Mechanism](#) specifies that requests must be made in writing and contain:

- any information that forms the basis for the request;
- a description of the nature of information or relief sought;
- a list of United States Government entities believed to be involved (if any); and
- any information about other measures pursued to obtain the information or relief requested and the response received through those other measures.

Information that forms the basis of the request should include unique identifiers associated with the types of communications an individual believes may have been accessed. For example, for concerns about email communications, a person will need to provide the relevant email addresses. Likewise, relevant telephone numbers must be provided if a person is concerned about telephone communications. Individuals can also include other information about the concerns that precipitated the request. Such information is requested in order to facilitate a precise and accurate review, and in general, more detailed requests may correspondingly enable a more detailed review.

A request does not need to demonstrate that the requester's data has been accessed by the United States Government through signal intelligence activities.

Information submitted to the Ombudsperson as part of a request for review will not be used or retained for other purposes unless necessary to comply with applicable law. The EU and Swiss

complaint handling bodies do not need to forward information provided for verifying the identity of the requestor or an individual's contact information.

**Additional Resources:**

[Privacy Shield Website](#)

[U.S.-EU Privacy Shield Framework Text](#)

[U.S.-Swiss Privacy Shield Framework Text](#)

[Ombudsperson Mechanism](#)

[Ombudsperson Mechanism Implementation Procedures \(UNCLASSIFIED\)](#)

[Presidential Policy Directive 28](#)

[ODNI Office of Civil Liberties, Privacy, and Transparency](#)

[Privacy and Civil Liberties Oversight Board](#)

[Freedom of Information Act \(FOIA\)](#)

[Privacy Act](#)

[European Commission Privacy Shield website](#)

[Swiss Federal Data Protection and Information Commissioner \(FDPIC\)](#)

## Attachment 7

### Statement by the Acting Director of FTC's Bureau of Consumer Protection Regarding Reported Concerns about Facebook Privacy Practices

FOR RELEASE

March 26, 2018

TAGS:

- [Technology](#)
- [Bureau of Consumer Protection](#)
- [Consumer Protection](#)
- [Privacy and Security](#)
- [Consumer Privacy](#)

Tom Pahl, Acting Director of the Federal Trade Commission's Bureau of Consumer Protection, issued the following statement regarding reported concerns about Facebook's privacy practices:

"The FTC is firmly and fully committed to using all of its tools to protect the privacy of consumers. Foremost among these tools is enforcement action against companies that fail to honor their privacy promises, including to comply with Privacy Shield, or that engage in unfair acts that cause substantial injury to consumers in violation of the FTC Act. Companies who have settled previous FTC actions must also comply with FTC order provisions imposing privacy and data security requirements. Accordingly, the FTC takes very seriously recent press reports raising substantial concerns about the privacy practices of Facebook. Today, the FTC is confirming that it has an open non-public investigation into these practices."

The Federal Trade Commission works to promote competition, and [protect and educate consumers](#). You can [learn more about consumer topics](#) and [file a consumer complaint online](#) or by calling 1-877-FTC-HELP (382-4357). Like the FTC on [Facebook](#), follow us on [Twitter](#), read our [blogs](#) and [subscribe to press releases](#) for the latest FTC news and resources.

CONTACT INFORMATION

---

MEDIA CONTACT:

[Peter Kaplan](#)

*FTC Office of Public Affairs*

202-326-2334



## Attachment 8

# FAQs - Onward Transfer Principle

The following FAQs are relevant to an organization preparing to come into compliance with the Accountability for Onward Transfer Principle.

***Q1: Are Privacy Shield participants required to have contracts in place when transferring data to controllers and agents?***

Generally speaking, yes. The [Accountability for Onward Transfer Principle](#) provides that a contract is required when personal data received under the Privacy Shield is transferred either to a third party acting as a controller or to a third party acting as an agent.

However, as explained in [Supplemental Principle 9\(e\)](#), 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 entering into a contract with the third-party controller, provided that the Privacy Shield organization has complied with the Notice and Choice Principles. Furthermore, when personal information is transferred between two controllers within a controlled group of corporations or entities, a contract is not always required, as explained in [Supplemental Principle 10\(b\)](#).

***Q2: Can standard contractual clauses be used to meet the Accountability for Onward Transfer Principle's contractual requirements?***

Yes. Organizations may use contracts that fully reflect the requirements of the relevant [standard contractual clauses adopted by the European Commission](#) to fulfill these contractual requirements, though neither the use of standard contractual clauses nor prior authorization of contracts is required under the Frameworks. Organizations are encouraged to consider the context of the transfer, their processing operations, and the needs of their business and customers in determining which contractual provisions are most appropriate.

Note: The European Commission has decided that [standard contractual clauses](#) offer sufficient safeguards on data protection for data to be transferred internationally. As such, they are also an alternative to Privacy Shield to facilitate transfers of personal data from the European Union to organizations in the United States.

**Q3: When transferring data to a third party, is a Privacy Shield participant obligated to require that third party to participate in Privacy Shield?**

No. [Supplemental Principle 10](#) specifies that the requirement to enter into a contract that provides the same level of protection does not require the third party controller to be a Privacy Shield organization. With regard to transfers to an agent, the [Accountability for Onward Transfer Principle](#) makes clear that a contract is required and states that the Privacy Shield participant must “ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles.” The Frameworks do not prescribe how an agent must be obligated to provide this level of protection. Privacy Shield participants have used different mechanisms to obligate third party agents to provide the same level of privacy protection, including specifying protections in the contract between the Privacy Shield participant and the agent, using an agent located in a country which has been found by the European Commission to ensure an adequate level of protection, using an agent that is subject to the EU data protection rules and using an agent that is a Privacy Shield participant.

**Q4: When transferring data to a third party, is a Privacy Shield participant obligated to require that third party to register with an independent recourse mechanism?**

No. [Supplemental Principle 10](#) specifies that when transfers are made to a controller, the recipient controller need not have an independent recourse mechanism, provided it makes available an “equivalent mechanism.” When transfers are made to an agent, the agent must be “obligated to provide at least the same level of **privacy protection** as is required by the Principles [emphasis added].” Third party recipients of data under the Privacy Shield have frequently used in-house dispute settlement procedures to provide an “equivalent mechanism.”

## FAQs - Processing Guidance

The following FAQs are relevant when personal data is transferred from the European Union (EU) to the United States for processing purposes only.

When responding to individuals seeking to exercise their rights under the Privacy Shield Principles, a processor should respond pursuant to the instructions of the EU data controller.

***Q1: When personal data is transferred from the European Union (EU) to the United States for processing purposes only, what contractual requirements are mandated by the Framework(s)?***

[Supplemental Principle 10a](#) of the EU-U.S. Privacy Shield Framework addresses this question (and is reproduced here in its entirety for ease of reference, given its relevance to the other FAQs below).

- i. When personal data is transferred from the EU to the United States only for processing purposes, a contract will be required, regardless of participation by the processor in the Privacy Shield.
- ii. Data controllers in the European Union are always required to enter into a contract when a transfer for mere processing is made, whether the processing operation is carried out inside or outside the EU, and whether or not the processor participates in the Privacy Shield. The purpose of the contract is to make sure that the processor:
  1. acts only on instructions from the controller;
  2. provides appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alternation, unauthorized disclosure or access, and understands whether onward transfer is allowed; and
  3. taking into account the nature of the processing, assists the controller in responding to individuals exercising their rights under the Principles.
- iii. Because adequate protection is provided by Privacy Shield participants, contracts with Privacy Shield participants for mere processing do not require prior authorization (or such authorization will be granted automatically by the EU Member States), as would be required for contracts with recipients not participating in the Privacy Shield or otherwise not providing adequate protection.

**Q2: How can a Privacy Shield participant acting as a processor adhere to the Frameworks' Notice Principle?**

The [Notice Principle](#) requires all Privacy Shield participants to inform individuals about thirteen discrete elements, including the following:

- the purposes for which it collects and uses personal information about them
- the choices and means the organization offers individuals for limiting the use and disclosure of their personal data
- the right of individuals to access their personal data

Organizations processing data only on the instructions of an EU controller frequently ask how they should address those three elements in their privacy policies.

Every Privacy Shield participant must inform individuals about all thirteen elements of the Notice Principle. Organizations processing data only on the instructions of an EU controller may choose to acknowledge that this is the function they are performing when informing individuals about these elements in their privacy policies. For instance, a processor could acknowledge that it processes data only on the instructions of an EU controller and describe the type of processing services it provides. Similarly, with respect to accessing data, a processor could provide individuals with its contact information, while noting that it will work with the EU controller to facilitate access or choice.

**Q3: How can a Privacy Shield participant acting as a processor adhere to the Frameworks' Choice Principle?**

The [Choice Principle](#) states, in part, that:

“An organization must offer individuals the opportunity to choose (opt out) whether their personal information is (i) to be 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 by the individuals. Individuals must be provided with clear, conspicuous, and readily available mechanisms to exercise choice.”

[Supplemental Principle 10a](#) provides that the processor acts only on instructions from the EU controller, which would include instructions regarding the Choice Principle and regarding how a mechanism to exercise choice would be provided. As an example, an organization acting as a processor with contractual limitations on disclosure or use of information could inform individuals about these contractual limitations on its ability to disclose personal information to third parties or to use personal information for purposes other than those specified in the contract. As another example, an organization acting as a processor could, pursuant to the EU controller's instructions, put individuals in contact with the controller that provides a choice mechanism or offer a choice mechanism directly.

***Q4: How can a Privacy Shield participant acting as a processor adhere to the Frameworks' Data Integrity and Purpose Limitation Principle?***

The [Data Integrity and Purpose Limitation Principle](#) states, in part:

“An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization must take reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current...”

“Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing .... This obligation does not prevent organizations from processing personal information for longer periods for the time and to the extent such processing reasonably serves the purposes of archiving in the public interest, journalism, literature and art, scientific or historical research, and statistical analysis ....”

When an organization acting as a processor is operating under contractual requirements governing data retention, accuracy and purposes of processing, it may have no direct contact with individuals to which the data pertains. In such a case, the processor should work with the EU controller to ensure that these requirements are met.

***Q5: How can a participant acting as a processor adhere to the Frameworks' Access Principle?***

The [Access Principle](#) states:

“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, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.”

When a Privacy Shield participant is acting as a processor, it should provide access by putting an individual in contact with the EU controller, or by working together with the EU controller to provide access, as prescribed by the EU controller.

**Attachment 9**

# **Statement by the Press Secretary on the EU – U.S. Privacy Shield**

**INFRASTRUCTURE & TECHNOLOGY** | Issued on: September 15, 2017

---

---

The White House applauds the preparation efforts in advance of the first annual joint review of the EU – U.S. Privacy Shield. We firmly believe that the upcoming review will demonstrate the strength of the American promise to protect the personal data of citizens on both sides of the Atlantic. This first-of-a-kind event brings together the expertise and resources of seven Federal agencies, hundreds of industry representatives, and other stakeholders to demonstrate the value and integrity of the Privacy Shield, which has noticeably improved transatlantic data protection practices.

The United States commitment to the Privacy Shield cannot be stronger. Programs like the Privacy Shield and the Asia-Pacific Economic Cooperation Cross-Border Privacy Rules system enable the free flow of information, which sustains the nearly \$1 trillion dollars in goods and services trade across the Atlantic, and even more around the globe. We look forward to a successful annual review and the continuation of our constructive partnership with the European Union on the Privacy Shield framework.



## Attachment 10

1.8.2016 EN

Official Journal of the European Union

L 207/1

### II

(Non-legislative acts)

## DECISIONS

### COMMISSION IMPLEMENTING DECISION (EU) 2016/1250 of 12 July 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**

*(notified under document C(2016) 4176)*

**(Text with EEA relevance)**

#### *3.2.1. Access and use by U.S. public authorities for law enforcement and public interest purposes*

(125) As regards interference with personal data transferred under the EU-U.S. Privacy Shield for law enforcement purposes, the U.S. government (through the Department of Justice) has provided assurance on the applicable limitations and safeguards which in the Commission's assessment demonstrate an adequate level of protection.

(126) According to this information, under the Fourth Amendment of the U.S. Constitution (179) searches and seizures by law enforcement authorities principally (180) require a court-ordered warrant upon a showing of 'probable cause'. In the few specifically established and exceptional cases where the warrant requirement does not apply (181), law enforcement is subject to a 'reasonableness' test (182). Whether a search or seizure is reasonable is 'determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests' (183). More generally, the Fourth Amendment guarantees privacy, dignity, and protects against arbitrary and invasive acts by officers of the Government (184). These concepts capture the idea of necessity and proportionality in Union law. Once law enforcement no longer has a need to use the seized items as evidence, they should be returned (185).

(127) While the Fourth Amendment right does not extend to non-U.S. persons that are not resident in the United States, the latter nevertheless benefit indirectly from its protections, given that the personal data are held by U.S. companies with the effect that law enforcement authorities in any event have to seek judicial authorisation (or at least respect the reasonableness requirement) (186). Further protections are provided by special statutory authorities, as well as the Department of Justice Guidelines, which limit law enforcement access to data on grounds equivalent to necessity and proportionality (e.g. by requiring that the FBI use the least intrusive investigative methods feasible, taking into account the effect on privacy and civil liberties) (187). According to the representations made by the U.S. government, the same or higher protections apply to law enforcement investigations at State level (with respect to investigations carried out under State laws) (188).

(128) Although a prior judicial authorisation by a court or grand jury (an investigate arm of the court impanelled by a judge or magistrate) is not required in all cases (189), administrative subpoenas are limited to specific cases and will be subject to independent judicial review at least where the government seeks enforcement in court (190).

(129) The same applies for the use of administrative subpoenas for public interest purposes. In addition, according to the representations from the U.S. government, similar substantive limitations apply in that agencies may only seek access to data that is relevant to matters falling within their scope of authority and have to respect the standard of reasonableness.

(130) Moreover, U.S. law provides for a number of judicial redress avenues for individuals, against a public authority or one of its officials, where these authorities process personal data. These avenues, which include in particular the Administrative Procedure Act (APA), the Freedom of Information Act (FOIA) and the Electronic Communications Privacy Act (ECPA), are open to all individuals irrespective of their nationality, subject to any applicable conditions.

(131) Generally, under the judicial review provisions of the Administrative Procedure Act (191), 'any person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action', is entitled to seek judicial review (192). This includes the possibility to ask the court to 'hold unlawful and set aside agency action, findings, and conclusions found to be [...] arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law' (193).

(132) More specifically, Title II of the Electronic Communications Privacy Act (194) sets forth a system of statutory privacy rights and as such governs law enforcement access to the contents of wire, oral or electronic communications stored by third-party service providers (195). It criminalises the unlawful (i.e. not authorised by court or otherwise permissible) access to such communications and provides recourse for an affected individual to file a civil action in U.S. federal court for actual and punitive damages as well as equitable or declaratory relief against a government official that has wilfully committed such unlawful acts, or against the United States.