Privacy Shield: Common and Supplementary Principles

This policy is comprised of the seven common principles of the Privacy Shield Program Framework and affirms Shift4's commitment to the program.

The Privacy Shield Program Framework also includes 16 equally binding principles that explain and augment the first seven. Shift4 confirms its eligibility under FTC jurisdiction, which covers acts or practices in or affecting commerce by any "person, partnership, or corporation."

This privacy policy, as updated, will be publicly maintained in the Shift4 Security Corner http://www.shift4.com/insight/security/.

The Privacy Shield Framework can be found at https://www.privacyshield.gov/welcome.

1. Overview

1.1. While the United States and the European Union share the goal of enhancing privacy protection, the United States takes a different approach to privacy from that taken by the European Union. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self-regulation. Given those differences and to provide organizations in the United States with a reliable mechanism for personal data transfers to the United States from the European Union while ensuring that EU data subjects continue to benefit from effective safeguards and protection as required by European legislation with respect to the processing of their personal data when they have been transferred to non-EU countries, the Department of Commerce is issuing these Privacy Shield Principles, including the Supplemental Principles (collectively "the Principles") under its statutory authority to foster, promote, and develop international commerce (15 U.S.C. § 1512). The Principles were developed in consultation with the European Commission, and with industry and other stakeholders, to facilitate trade and commerce between the United States and European Union. They are intended for use solely by organizations in the United States receiving personal data from the European Union for the purpose of qualifying for the Privacy Shield and thus benefitting from the European Commission's adequacy decision. The Principles do not affect the application of national provisions implementing Directive 95/46/EC ("the Directive") that apply to the processing of personal data in the Member States. Nor do the Principles limit privacy obligations that otherwise apply under U.S. law.

1.2. In order to rely on the Privacy Shield to effectuate transfers of personal data from the EU, an organization must self-certify its adherence to the Principles to the Department of Commerce (or its designee) ("the Department"). While decisions by organizations to thus enter the Privacy Shield are entirely voluntary, effective compliance is compulsory: organizations that self-certify to the Department and publicly declare their commitment to adhere to the Principles must comply

fully with the Principles. In order to enter the Privacy Shield, an organization must (a) be subject to the investigatory and enforcement powers of the Federal Trade Commission (the "FTC"), the Department of Transportation or another statutory body that will effectively ensure compliance with the Principles (other U.S. statutory bodies recognized by the EU may be included as an annex in the future); (b) publicly declare its commitment to comply with the Principles; (c) publicly disclose its privacy policies in line with these Principles; and (d) fully implement them. An organization's failure to comply is enforceable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts in or affecting commerce (15 U.S.C. § 45(a)) or other laws or regulations prohibiting such acts.

1.3. The Department of Commerce will maintain and make available to the public an authoritative list of U.S. organizations that have self-certified to the Department and declared their commitment to adhere to the Principles ("the Privacy Shield List"). Privacy Shield benefits are assured from the date that the Department places the organization on the Privacy Shield List. The Department will remove an organization from the Privacy Shield List if it voluntarily withdraws from the Privacy Shield or if it fails to complete its annual re-certification to the Department. An organization's removal from the Privacy Shield List means it may no longer benefit from the European Commission's adequacy decision to receive personal information from the EU. The organization must continue to apply the Principles to the personal information it received while it participated in the Privacy Shield, and affirm to the Department on an annual basis its commitment to do so, for as long as it retains such information; otherwise, the organization must return or delete the information or provide "adequate" protection for the information by another authorized means. The Department will also remove from the Privacy Shield List those organizations that have persistently failed to comply with the Principles; these organizations do not qualify for Privacy Shield benefits and must return or delete the personal information they received under the Privacy Shield.

1.4. The Department will also maintain and make available to the public an authoritative record of U.S. organizations that had previously self-certified to the Department, but that have been removed from the Privacy Shield List. The Department will provide a clear warning that these organizations are not participants in the Privacy Shield; that removal from the Privacy Shield List means that such organizations cannot claim to be Privacy Shield compliant and must avoid any statements or misleading practices implying that they participate in the Privacy Shield; and that such organizations are no longer entitled to benefit from the European Commission's adequacy decision that would enable those organizations to receive personal information from the EU. An organization that continues to claim participation in the Privacy Shield or makes other Privacy Shield-related misrepresentations after it has been removed from the Privacy Shield List may be subject to enforcement action by the FTC, the Department of Transportation, or other enforcement authorities.

1.5. Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that creates conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.

1.6. Organizations are obligated to apply the Principles to all personal data transferred in reliance on the Privacy Shield after they enter the Privacy Shield. 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 to the Department and conform to the requirements set forth in the Supplemental Principle on Self-Certification.

1.7. U.S. law will apply to questions of interpretation and compliance with the Principles and relevant privacy policies by Privacy Shield organizations, except where such organizations have committed to cooperate with European data protection authorities ("DPAs"). Unless otherwise stated, all provisions of the Principles apply where they are relevant.

1.8. Definitions:

1.8.1. "Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by an organization in the United States from the European Union, and recorded in any form.

1.8.2. "Processing" of personal data means any operation or set of operations which is performed upon personal data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

1.8.3. "Controller" means a person or organization which, alone or jointly with others, determines the purposes and means of the processing of personal data.

2. Notice

2.1. An organization must inform individuals about:

2.1.1. Its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List.

The Privacy Shield List can be found at https://www.privacyshield.gov/list.

2.1.2. The types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles.

Shift4 processes, stores, and transmits cardholder data in compliance with the internationally recognized Payment Card Industry Data Security Standard (PCI DSS) and the terms, requirements, and definitions contained within the merchant services agreements Shift4 executes with its merchants and partners.

2.1.3. Its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield.

Shift4 Corporation sets forth this policy as affirmation of its commitment to the Principles of the Privacy Shield.

2.1.4. The purposes for which it collects and uses personal information about them.

Shift4 is a payment gateway, payment services provider, and processor that performs credit card authorization and settlement services for merchants. Cardholder data is electronically collected through secure channels, securely stored, and securely transmitted to other processors in accordance with the terms contained in the merchant services agreements it makes with merchants. Upon retirement, cardholder data is securely destroyed in accordance with the respective data retention instructions detailed in the merchant services agreements and/or individually configured via a Shift4 portal as part of the solution provided to the merchant.

2.1.5. How to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints.

Inquiries or complaints may be submitted to the Shift4 Security Compliance Officer by emailing PCI@shift4.com or by calling 702.597.2480, ext. 46700.

2.1.6. The type or identity of third parties to which it discloses personal information, and the purposes for which it does so.

Shift4, under written contracts and service level agreements, shares cardholder data with payment card processors and with the credit card brands, associated with the Payment Card Industry, under their respective operating rules.

2.1.7. The right of individuals to access their personal data.

This process must be initiated with the merchant that initially collected, or directed the collection of the personal data. Personal data will not be retrievable if the date of the request is past its retirement date.

2.1.8. The choices and means the organization offers individuals for limiting the use and disclosure of their personal data.

Shift4 processes, stores, and transmits cardholder data in compliance with the internationally recognized PCI Data Security Standard (PCI DSS). Other than authorization and settlements services, cardholder data is never used for any other purpose and is never disclosed to or shared with third parties not directly involved with payment processing or acquiring.

2.1.9. The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by Data Protection Authorities (DPAs), (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States.

Shift4 commits to cooperate with the DPAs by declaring in its Privacy Shield self-certification submission to the Department of Commerce (see Supplemental Principle on Self-Certification) that it:

> **i.** elects to satisfy the requirement in points (a)(i) and (a)(iii) of the Privacy Shield Recourse, Enforcement and Liability Principle found here by committing to cooperate with the DPAs;
>
> **ii.** will cooperate with the DPAs in the investigation and resolution of complaints brought under the Privacy Shield; and
>
> **iii.** will comply with any advice given by the DPAs where the DPAs take the view that the organization needs to take specific action to comply with the

Privacy Shield Principles, including remedial or compensatory measures for the benefit of individuals affected by any non-compliance with the Principles, and will provide the DPAs with written confirmation that such action has been taken

2.1.10. Being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body.

2.1.11. The possibility, under certain conditions, for the individual to invoke binding arbitration.

2.1.12. The requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

2.1.13. Its liability in cases of onward transfers to third parties.

2.2. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

3. Choice

3.1. 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.

3.2. By derogation to the previous paragraph, it is not necessary to provide choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. However, an organization shall always enter into a contract with the agent.

3.3. 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), organizations must obtain affirmative express consent (opt in) from individuals if such information is to be (i) disclosed to a third party or (ii) used for a purpose other than those for which it was originally collected or subsequently authorized by the individuals through the exercise of opt-in choice. In

addition, an organization should treat as sensitive any personal information received from a third party where the third party identifies and treats it as sensitive.

4. Accountability for Onward Transfer

4.1. To transfer personal information to a third party acting as a controller, organizations must comply with the Notice and Choice Principles. Organizations must also enter into a contract with the third-party controller that provides 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 the Principles and will notify the organization if it makes a determination that it can no longer meet this obligation. The contract shall provide that when such a determination is made the third party controller ceases processing or takes other reasonable and appropriate steps to remediate.

Shift4 acknowledges its accountability for the onward transfer of individuals' data to third parties, pursuant to the Privacy Shield principles. Shift4 further acknowledges that it may be liable should the data not be used consistent with agreed-upon contracts.

4.2. To transfer personal data to a third party acting as an agent, organizations must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

5. Security

5.1 Organizations creating, maintaining, using, or disseminating personal information must take reasonable appropriate measures to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into due account the risks involved in the processing and the nature of the personal data.

Shift4 processes, stores, and transmits cardholder data in compliance with the internationally recognized PCI Data Security Standard (DSS). Shift4's internal security controls are assessed annually by an independent, PCI Qualified Security Assessor, and have been consistently judged far above the minimum standards called out in the PCI DSS.

6. Data Integrity and Purpose Limitation

6.1. Consistent with the Principles, 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 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. An organization must adhere to the Principles for as long as it retains such information.

6.2. Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose of processing within the meaning of 6.1. 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. In these cases, such processing shall be subject to the other Principles and provisions of the Framework. Organizations should take reasonable and appropriate measures in complying with this provision.

7. Access

7.1. 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.

8. Recourse, Enforcement, and Liability

8.1. 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. At a minimum such mechanisms must include:

8.1.1. Readily available independent recourse mechanisms by which each individual's complaints and disputes are investigated and expeditiously resolved at no cost to the individual and by reference to the Principles, and damages awarded where the applicable law or private-sector initiatives so provide;

8.1.2. Follow-up procedures for verifying that the attestations and assertions organizations make about their privacy practices are true and that privacy practices have been implemented as presented and, in particular, with regard to cases of non-compliance; and

8.1.3. Obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.

8.2. Organizations and their selected independent recourse mechanisms will respond promptly to inquiries and requests by the Department for information relating to the Privacy Shield. All organizations must respond expeditiously to complaints regarding compliance with the Principles referred by EU Member State authorities through the Department. Organizations that have chosen to cooperate with DPAs, including organizations that process human resources data, must respond directly to such authorities with regard to the investigation and resolution of complaints.

8.3. Organizations are obligated to arbitrate claims and follow the terms as set forth in Annex I, provided that an individual has invoked binding arbitration by delivering notice to the organization at issue and following the procedures and subject to conditions set forth in Annex I.

8.4. In the context of an onward transfer, a Privacy Shield organization has responsibility for the processing of personal information it receives under the Privacy Shield and subsequently transfers to a third party acting as an agent on its behalf. The Privacy Shield organization shall remain liable under the Principles if its agent processes such personal information in a manner inconsistent with the Principles, unless the organization proves that it is not responsible for the event giving rise to the damage.

8.5. When an organization becomes subject to an FTC or court order based on non-compliance, the organization shall make public any relevant Privacy Shield-related sections of any compliance or assessment report submitted to the FTC, to the extent consistent with confidentiality requirements. The Department has established a dedicated point of contact for DPAs for any problems of compliance by Privacy Shield organizations. The FTC will give priority consideration to referrals of non-compliance with the Principles from the Department and EU Member State authorities, and will exchange information regarding referrals with the referring state authorities on a timely basis, subject to existing confidentiality restrictions.

9. Supplemental Principles

9.1. In addition to the seven principles, there are 16 supplemental principles that Shift4 subscribes to, which are listed here. This includes completing and maintaining a self-assessment of the Privacy Shield Framework.

10. Supplemental Principle 7c

10.1 Shift4 chooses to certify its commitment to the Privacy Shield Principles under the provisions of Supplemental Principle 7c – Self-Assessment approach.