WILMERHALE

# Comparison of Requirements Under the Privacy Shield/Safe Harbor Principles

JULY 25, 2016

| Privacy Principle | Safe Harbor | Privacy Shield |
|---|---|---|
| | | Similar to the prior regime, an organization must provide information about the following in its privacy policy:<br>– its participation in the Privacy Shield and a web address for the Privacy Shield List<br>– the purposes for which it collects and uses personal data<br>– how to contact the self-certified organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints<br>– the type or identity of third parties to which it discloses personal data, and the purposes for which it does so<br>– the choices and means the organization offers individuals for limiting the use and disclosure of their personal |

**Notice Requirements**

The Privacy Shield notice requirements are more specific and detailed than what was required by the Safe Harbor regime. Safe Harbor required a privacy policy to provide information on data processing activities and address conformity with the Safe Harbor's privacy principles, but the Privacy Shield imposes a number of specific new additions.

An organization must provide information about the following in its privacy policy:

- its adherence to the Safe Harbor principles
- the purposes for which it collects and uses personal data
- how to contact the organization with any inquiries or complaints
- the types of third parties to which the organization discloses personal data
- the choices and means that the organization offers individuals for limiting the use and disclosure of their personal data
- the independent recourse mechanism(s) available to investigate unresolved complaints and relevant contact information for that mechanism
- the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, whether that body is established by data protection authorities, and whether that body is based in the EU or the United States

An organization's privacy policy must also address:

- the right of individuals to access their personal data
- the types of personal data collected
- any entities or subsidiaries of the organization also adhering to the Privacy Shield principles
- the organization's commitment to subject itself to the Privacy Shield for all personal data transferred from the EU in reliance on the Privacy Shield
- how the organization is subject to the investigatory and enforcement powers of the FTC, Department of Transportation, or another US authorized statutory body
- the possibility, under certain conditions, for the individual to invoke binding arbitration
- the requirement to disclose personal data in response to lawful requests by public authorities

| | | |
|---|---|---|
| | | – the organization's liability in cases of onward transfers to third parties<br>The notice must be provided when individuals are first asked to provide personal data or as soon thereafter as practicable, and always before the organization uses such information for a new purpose or discloses it to a third party. |
| **Choice Requirements**<br><br>The Privacy Shield does not change the Safe Harbor's choice principle. | Organizations must offer an opt-out where personal data is (1) disclosed to non-agent third parties or (2) used for a materially different purpose than that for which it was originally collected or subsequently authorized by the individual. An opt-in must be provided for sensitive data. | Organizations must offer an opt-out where personal data is (1) disclosed to non-agent third parties or (2) used for a materially different purpose than that for which it was originally collected or subsequently authorized by the individual. An opt-in must be provided for sensitive data.<br><br>*Third Parties acting as Data Controllers:* The Privacy Shield's notice and choice principles apply, requiring an opt-in or opt-out depending upon the use or type of data. Organizations must also contract with such third parties, obligating the third-party data controller to:<br><br>– Process data only "for limited and specified purposes" consistent with the consent provided by the individual<br>– Provide the same level of protection as the Privacy Shield principles<br>– Notify the organization if it cannot meet this obligation, |
| | *Third Parties acting as Data Controllers:* | |

| | | |
|---|---|---|
| | The Safe Harbor's notice and choice principles apply, requiring an opt-in or opt-out depending upon the use or type of data. | and then cease processing or take other steps to remediate<br><br>*Third Parties acting as Agents/Vendors "to perform task(s) on behalf of and under the instructions" of an organization:* Organizations must:<br><br>– Transfer personal data only for limited and specified purposes<br>– Ascertain that the agent is required to provide the same level of protection as the Privacy Shield principles<br>– Take steps to ensure that the agent effectively processes personal data consistent with the organization's Privacy Shield obligations<br>– Require the agent to notify the organization if the agent can no longer meet its obligations<br>– Upon such notice, take steps to stop and remediate unauthorized processing<br>– Provide information about relevant contractual provisions to the Department of Commerce upon request<br><br>The organization must enter into a contract with the agent ensuring compliance with these obligations. Where a third-party agent violates the Privacy Shield principles, the Privacy Shield places the obligation on certified organizations to prove that they are not responsible for the event giving rise to the damage. |
| **Onward Transfers/Vendor Agreements**<br><br>The Privacy Shield imposes new requirements (and liability for) onward transfers of data to third parties. | *Third Parties acting as Agents/Vendors "to perform task(s) on behalf of and under the instructions" of an organization:* Organizations must either (1) ascertain that the third-party agent is a Safe Harbor member or subject to an EU adequacy finding, or (2) enter into a contract requiring the agent to provide "at least the same level of privacy protection" as the Safe Harbor framework. If an organization complies with this, it will not be held liable if a third party processes information "in a way contrary to any restrictions or representations." | |

| | | |
|---|---|---|
| **Security**<br><br>The Privacy Shield does not change the Safe Harbor's security principle. | Organizations must implement "reasonable and appropriate" security measures, taking into account the risks involved in the processing and the nature of the personal data. | Organizations must implement "reasonable and appropriate" security measures, taking into account the risks involved in the processing and the nature of the personal data. |
| **Data Integrity/Purpose Limitation**<br><br>The Privacy Shield maintains the Safe Harbor's data integrity principle, but includes more detail on compatible purposes and includes new language on data retention and obligations to protect | Personal data "must be relevant for the purposes for which it is to be used," and organizations may not process information in ways "incompatible with the purpose for which it has been collected or subsequently authorized." Organizations must take "reasonable steps" to ensure that data is reliable for its intended use, accurate, complete, and current. | *Purpose Limitation:* Collection of personal data must be "limited" to that which is "relevant for the purposes of processing," and organizations may not process information in ways "incompatible with the purpose for which it has been collected or subsequently authorized by the individual."<br><br>– "Compatible processing purposes" depend on circumstances, but could include those "that reasonably serve customer relations, compliance and legal considerations, auditing, security and fraud prevention, preserving or defending the organization's legal rights, or other purposes consistent with the expectations of a reasonable person given the context of the collection."<br><br>*Data Retention:* The Privacy Shield principles also include language imposing a data retention limit: "Information may be retained in a form identifying or making identifiable the individual only for as long as it serves a purpose [consistent with the purpose limitation principle]."<br><br>*Ongoing Obligations:* The new framework explicitly states that, even if |

| | | |
|---|---|---|
| | | an organization terminates its certification in Privacy Shield, the organization remains bound by the Privacy Shield principles with respect to any personal data it retains that was collected under the Privacy Shield. Organizations must continue to affirm their commitment to apply the principles to any retained data.<br><br>*Data Integrity:* Organizations must take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current. |
| **Access, Correction, and Deletion Rights**<br><br>The Privacy Shield maintains the Safe Harbor's access principle, including the rights to amend, correct, or delete inaccurate data. The Privacy Shield augments these rights, enabling data subjects to correct, amend, or delete even accurate personal data where such information is processed in violation of the Privacy Shield principles. | Individuals must have access to personal<br>data that the organization has about them, and be allowed to correct, amend, or delete inaccurate personal data held by an organization, 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 other persons would be violated. No justification is required, and companies may not charge excessive fees for such access. | Individuals must have access to personal data that the organization has about them, and be allowed to correct, amend, or delete inaccurate personal data held by an organization, 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 other persons would be violated. Specific grounds for rejecting access are explored in the Supplemental Principles. No justification is required, and companies may not charge excessive fees for such access. The Privacy Shield also makes clear that amendment, correction, and deletion rights must be provided in circumstances where accurate personal data has been processed in violation of the framework.<br><br>Before self-certifying, companies must implement processes for handling complaints from EU data subjects, including a point of contact for |

| | | |
|---|---|---|
| | | complaints, and must ensure that an independent recourse mechanism is in place.<br><br>More specifically:<br><br>– EU data subjects who believe their data has been misused may complain directly to the Privacy Shield company, which must respond within 45 days<br>– Privacy Shield companies must either provide an independent recourse mechanism **free of charge** to EU data subjects or agree to submit to oversight by EU data protection authorities<br>– EU data subjects may complain to their home data protection authority, and DPAs remain free to submit complaints directly with the Department of Commerce. Companies are required to promptly respond to inquiries and requests about their compliance from US regulators<br>– As a matter of "last resort," EU data subjects may invoke binding arbitration by a "Privacy Shield Panel" composed of arbitrators designed by the Department of Commerce and European Commission<br>– Individuals (and companies) can seek judicial review and enforcement of arbitral decisions under the Federal |
| **Recourse, Enforcement and Liability**<br><br>The Privacy Shield creates far stronger enforcement obligations and establishes new recourse mechanisms. | – Under Safe Harbor, organizations were encouraged to have EU citizens raise complaints directly with the organization<br>– Companies also had to provide an affordable independent recourse mechanism<br>– The FTC committed to reviewing referrals from independent recourse mechanisms and EU Member States alleging non-compliance with the Safe Harbor | |

Arbitration Act

## Additional Obligations

- Organizations must make public any Privacy Shield-related sections of a compliance report or assessment submitted to the FTC if subject to an FTC or court order for non-compliance with the Privacy Shield Principles, to the extent consistent with confidentiality laws and rules
- Organizations must respond promptly to inquiries and requests by the Department of Commerce for information relating to their Privacy Shield compliance