

the Directive sets forth EU requirements for privacy and the protection of personal data. Among other things, it requires EU Member States to implement legislation that prohibits the transfer of personal data outside the EU, with exceptions, unless the European Commission has made a determination that the recipient jurisdiction's laws ensure the protection of such personal data. This determination is referred to commonly as meeting the EU's "adequacy" standard.

6. To satisfy the EU adequacy standard for certain commercial transfers, Commerce and the European Commission negotiated the EU-U.S. Privacy Shield framework, which went into effect in July 2016. The EU-U.S. Privacy Shield framework allows companies to transfer personal data lawfully from the EU to the United States. To join the EU-U.S. Privacy Shield framework, a company must self-certify to Commerce that it complies with the Privacy Shield Principles and related requirements that have been deemed to meet the EU's adequacy standard. Any company that voluntarily withdraws or lets its self-certifications lapse must take steps to affirm to Commerce that it is continuing to protect the personal information it received while it participated in the program.
7. Companies under the jurisdiction of the FTC, as well as the U.S. Department of Transportation, are eligible to join the EU-U.S. Privacy Shield framework. A company under the FTC's jurisdiction that claims it has self-certified to the Privacy Shield Principles, but failed to self-certify to Commerce, may be subject to an enforcement action based on the FTC's deception authority under Section 5 of the FTC Act.
8. Commerce maintains a public website, <https://www.privacyshield.gov/welcome>, where it posts the names of companies that have self-certified to the EU-U.S. Privacy Shield framework. The listing of companies, <https://www.privacyshield.gov/list>, indicates whether the company's self-certification is current.
9. Through at least June 2018, Respondent has disseminated or caused to be disseminated privacy policies and statements on the <http://www.smartstartemploymentscreeninginc.com/EmploymentScreening/PrivacyStatement-BackgroundCheckEmploymentScreening.asp> website, including, but not limited to, the following statements:

Participation in the EU-US Privacy Shield

SmartStart Employment Screening, Inc. complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. SmartStart has certified that it adheres to the Privacy Shield Principles of Notice, Choice, Accountability for Onward Transfer, Security, Data Integrity and Purpose Limitation, Access, and Recourse, Enforcement and Liability. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles,

the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification page, please visit <https://www.privacyshield.gov/>

Smart Start has joined the EU Privacy Shield Program and complies with the EU – US Privacy Shield Principles as it relates to the collection, use and retention of personal information from European Union member countries. SmartStart adheres to each of the Privacy Shield Principles with respect data received from the EU in reliance of the Privacy Shield: Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability as explained below.

10. Although Respondent obtained Privacy Shield certification in September 2016, it did not complete the steps necessary to renew its participation in the EU-U.S. Privacy Shield framework after that certification expired in September 2017, nor did it withdraw and affirm its commitment to protect any personal information it had acquired while in the program. After allowing its certification to lapse Respondent has continued to claim, as indicated in Paragraph 9, that it participates in the Privacy Shield program.

Count 1 – Privacy Misrepresentation

11. As described in Paragraph 9, Respondent represents, directly or indirectly, expressly or by implication, that it is a current participant in the EU-U.S. Privacy Shield Principles.
12. In fact, as described in Paragraph 10, Respondent is not a current participant in the EU-U.S. Privacy Shield Principles. Therefore, the representation set forth in Paragraph 11 is false or misleading.

Count 2 – Misrepresentation Regarding Continuing Obligations

13. As described in Paragraph 6, Respondent represented that it would abide by the EU-U.S. Privacy Shield framework principles. These principles include a requirement that if it ceased to participate in the EU-U.S. Privacy Shield framework, it must affirm to Commerce that it will continue to apply the principles to personal information that it received during the time it participated in the program.
14. In fact, as described in Paragraph 10, Respondent has not affirmed to Commerce that it will continue to apply the principles to personal information that it received during the time it participated in the program. Therefore, the representation set forth in Paragraph 13 is false or misleading.

Violations of Section 5 of the FTC Act

15. The acts and practices of Respondent as alleged in this complaint constitute deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

THEREFORE, the Federal Trade Commission this fifteenth day of November 2018, has issued this complaint against Respondent.

By the Commission, Commissioner Wilson not participating.

Donald S. Clark
Secretary

SEAL: