

Draft

Frequently Asked Questions (FAQs)

FAQ 11: Dispute Resolution and Enforcement⁽¹⁾

Q: How should the the dispute resolution requirements of the enforcement principle be implemented, and how will an organization's persistent failure to comply with the principles be handled?

A: The enforcement principle sets out the criteria for safe harbor

enforcement mechanisms. These mechanisms may take different forms, but they must meet the enforcement principle's requirements. Organizations may satisfy the requirements set forth in this principle through the following: (1) compliance with private sector developed privacy programs that incorporate the safe harbor principles into their rules and which include effective enforcement mechanisms of the type described in the enforcement principle; (2) compliance with legal or regulatory supervisory authorities; or (3) by committing to cooperate with data protection authorities located in the European Community or their authorized representatives [, provided those authorities agree].⁽²⁾ This list is intended to be illustrative and not limiting. The private sector may design other mechanisms to provide enforcement, so long as they meet the requirements of the principles and the FAQs.

Recourse Mechanisms. Consumers should be encouraged to raise any complaints they may have with the relevant organization before proceeding to independent recourse mechanisms. Whether a recourse mechanism is independent is a factual question that can be demonstrated in a number of ways, for example, by transparent composition and financing or a proven track record. As noted, the recourse available to individuals should be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous or do not meet the eligibility requirements established by the organization operating the recourse mechanism. In addition, they should provide individuals with information about how the dispute resolution procedure works when they file a complaint.

Remedies and Sanctions. The result of any remedies provided by the dispute resolution body should be that individuals are assured that future processing by the organization of their data will be in conformity with the principles or that processing of the individual's personal data will cease.

Sanctions need to be rigorous enough to ensure compliance by the organization with the principles. These can include suspension and removal of a seal, injunctive orders, deletion of relevant data, and/or publicity for negative findings. Dispute resolution bodies or self regulatory bodies are encouraged to refer failures of organizations to comply with their rulings to courts or to the governmental body with applicable jurisdiction, as appropriate.

FTC Action. The FTC has committed to reviewing on a priority basis referrals received from privacy self regulatory organizations, such as BBOnline and TRUSTe, and EU member countries alleging non-compliance with the safe harbor principles to determine whether Section 5 of the FTC Act prohibiting unfair or deceptive acts or practices in commerce has been violated. If the FTC concludes that it has reasons to believe Section 5 has been violated, it may resolve the matter by seeking an administrative cease and desist order prohibiting the challenged practices or by filing a complaint in federal district court, which if successful could result in a federal court order to same effect. The FTC may obtain civil penalties for violations of an administrative cease and desist order and may pursue civil or criminal contempt for violation of a federal court order. The FTC will notify the Department of Commerce of any such actions it takes. The Department of Commerce encourages other government bodies and safe harbor organizations to notify it of the final disposition of any such referrals or other rulings determining adherence to the safe harbor principles.

Persistent Failure to Comply. The Department (or its designee) will indicate on the public list it maintains of organizations self certifying to the safe harbor any notification it receives from any dispute resolution, self regulatory, and/or government bodies of any persistent failure of any safe harbor organization to comply with the safe harbor principles or any decision of such bodies, but only after first providing thirty (30) days' notice to such organization and an opportunity to respond.

1. The EC received this FAQ on November 12 and is in the process of reviewing it with respect to its overall enforcement concerns and more particularly deletion of data when processed in violation of the principles, an issue raised by the EC in connection with the access principles.

2. See EC reserve on FAQ 5.