

## Draft

## Frequently Asked Questions (FAQs)

## FAQ No 11: Dispute Resolution and Enforcement

*Q.11: How should 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.11: The enforcement principle sets out the requirements for safe harbor enforcement. How to meet the requirements of point (b) of the principle is set out in the FAQ on verification (FAQ 7). This FAQ 11 addresses points (a) and (c), both of which require independent recourse mechanisms. These mechanisms may take different forms, but they must meet the enforcement principle's requirements. Organizations may satisfy the requirements through the following: (1) compliance with private sector developed privacy programs that incorporate the safe harbor principles into their rules and ~~which~~that include effective enforcement mechanisms of the type described in the enforcement principle; (2) compliance with legal or regulatory supervisory authorities that provide for handling of individual complaints and dispute resolution; or (3) commitment to cooperate with data protection authorities located in the European Community or their authorized representatives, provided those authorities agree. 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 enforcement principle and the FAQs. Please note that the enforcement principle's requirements are additional to the requirement set forth in ~~the last sentence of the third~~ paragraph 3 of the introduction to the principles that self regulatory efforts must be enforceable under Section 5 of the Federal Trade Commission Act or similar statute.

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 required by the enforcement principle, the recourse available to individuals must be readily available and affordable. Dispute resolution bodies should look into each complaint received from individuals unless they are obviously unfounded or frivolous. This does not preclude the establishment of eligibility requirements by the organization operating the recourse mechanism, but such requirements should be transparent and justified (for example to exclude complaints that fall outside the scope of the program or are for consideration in another forum), and should not have the effect of undermining the commitment to look into legitimate complaints. In addition, recourse mechanisms should provide individuals with full and readily available information about how the dispute resolution procedure works when they file a complaint. Such information should include notice about the mechanism's privacy practices, in

conformity with the safe harbor principles.<sup>1</sup> They should also co-operate in the development of tools such as standard complaint forms to facilitate the complaint resolution process.

Remedies and Sanctions. The result of any remedies provided by the dispute resolution body should be that the effects of noncompliance are reversed or corrected by the organization, in so far as feasible, and that future processing by the organization will be in conformity with the principles and, where appropriate, that processing of the personal data of the individual who has brought the complaint will cease. Sanctions need to be rigorous enough to ensure compliance by the organization with the principles. A range of sanctions of varying degrees of severity will allow dispute resolution bodies to respond appropriately to varying degrees of non-compliance. Sanctions should include both publicity for findings of non-compliance and the requirement to delete data in certain circumstances.<sup>2</sup> Other sanctions could include suspension and removal of a seal, compensation for individuals for losses incurred as a result of non-compliance and injunctive orders. Private sector dispute resolution bodies and self regulatory bodies ~~should~~ must notify failures of safe harbor organizations to comply with their rulings to ~~courts or to~~ the governmental body with applicable jurisdiction or to the courts, as appropriate, and to notify the Department of Commerce (or its designee).

FTC Action. The FTC has committed to reviewing on a priority basis referrals received from privacy self regulatory organizations, such as BBBOnline 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 reason[s] 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 a 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 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. If an organization persistently fails to comply with the principles, it is no longer entitled to benefit from the safe harbor. Persistent failure to comply arises where an organization that has self certified to the Department of Commerce (or its designee) refuses to comply with a final determination by any self regulatory or government body or where such a body determines that an organization frequently fails to comply with the principles to the point where its claim to comply is no longer credible. In these cases, the organization must promptly notify the Department of Commerce (or its designee) of such facts. Failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).

The Department (or its designee) will indicate on the public list it maintains of organizations self certifying adherence to the safe harbor principles any notification it receives of persistent failure to comply, whether it is received from the organization itself, from a self regulatory body, or from a government body, but only after first providing thirty (30) days' notice and an opportunity to respond to the organization that has failed to comply. Accordingly, the public list maintained by the

Department of Commerce (or its designee) will make clear which organizations are assured and which organizations are no longer assured of safe harbor benefits.

An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the safe harbor must provide that body with full information about its prior participation in the safe harbor.

**1. Dispute resolution bodies are not required to conform with the enforcement principle. They may also derogate from the principles where they encounter conflicting obligations or explicit authorizations in the performance of their specific tasks.**

**2. Dispute resolutions bodies have discretion about the circumstances in which they use these sanctions. The sensitivity of the data concerned is one factor to be taken into consideration in deciding whether deletion of data should be required, as is whether an organization has collected, used or disclosed information in blatant contravention of the principles.**