CEOE COMMENTS ON THE REVISION OF THE SAFE HARBOUR FOR PERSONAL DATA TRANSFERS TO THE US

CEOE is looking forward to and supports the thorough analysis the European Commission has announced with regard to the Safe Harbour Agreement, especially considering that the previous European Commission (EC) Reports on the application of the Safe Harbour Agreement already had raised some important shortcomings. The problems identified then by the EC have not been rectified and represent a significant risk to consumers.

CEOE would like to put on the table some first baseline concepts regarding serious flaws in the implementation of the Safe Harbour that need to be addressed as soon as possible:

- **Scope.**
  The material scope is unclear as the definition included in Annex I of the EC Decision[1] does not define personal data in the same way than the Directive (95/46/EC). This creates considerable legal uncertainties on the scope of application. The definitions should be aligned.

  The agreement excludes certain sectors as e.g. the telecommunications and financial sectors as they are not subject to the jurisdiction of the Federal Trade Commission or the US Department of Transportation. This is in clear conflict to the most important plea of telecommunication operators regarding the need for a level playing field. This level playing field should be achieved not only between sectors, but also between EU and US companies.

  This is especially important considering that when the SH Principles were agreed in 2000, companies covered by the Agreement were not competing directly with telecommunication operators as it is the case today.

- **Enforcement.**
  The issue of a level playing field between EU and US players is even more challenged as long as effective enforcement is not sufficiently taking place in the US. The lack of enforcement actions means that US companies operate under a less stringent data protection standard and can process personal data of European citizens in ways that are forbidden to European companies without risking sanctions.

  The previous argument is reinforced if it is also considered the possibility of "onward transfer" - Transfers to Third Parties- (3rd Safe Harbour Principle) by which US companies can transfer data with much less restrictions than their European counterparts. This constitutes a clear discrimination of European companies and is affecting the competitiveness of European companies.

  The lack of enforcement has so far been observed by several independent studies (e.g. the Galexia study "safe harbour – fact or fiction?").

- **Transparency.**
  In a self-regulatory system, one of the key elements is transparency vis-à-vis the consumers. A simple self-certification scheme without any kind of monitoring by the Department of Commerce has not proved to be sufficient if some registered companies do not even comply with the most basic requirements of the Safe Harbour framework. Companies that falsely claim they do comply with the Safe Harbour Principles or they have been certified by the EU Safe Harbour mislead consumers and put the privacy of EU citizens at a risk.

  As a result, the European Commission should address these flaws by using its powers under Art.3 (4) and Art.4 of its underlying Decision including the modification or suspension of the Agreement.

[1] EC Decision 520/2000/EC of 26 July 2000 on the adequate protection of personal data provided by the Safe Harbour Privacy Principles, published in the Official Journal L 215, 25.08.2000