diritto&diritti dal 1996
diritto.it
direttore Francesco Brugaletta

ISSN 1127-8579

Pubblicato dal 11/12/2013

All'indirizzo http://www.diritto.it/docs/35757-business-and-personal-data-transfers-from-eu-to-us-safe-harbour-reloaded

Autore: Marcoccio Gloria

Business and personal data transfers from EU to US - Safe Harbour reloaded?

Business and personal data transfers from EU to US - Safe Harbour reloaded?

Gloria Marcoccio - gloria.marcoccio@glory.it

December 6, 2013

Background

Snowden recent revelations have turned on some lights about the U.S. mass surveillance programs based on the personal data of EU citizens collected by U.S. companies for the operation of their services ranging from Social Network contexts to commercial activities in many business sectors.

Without any claim to make assessments on such a complex and critical issue (for example: what we really know about similar mass surveillance programs conducted by police agencies of EU countries or of other Countries in the world, based on the on-line activities of EU citizens), it is definitely true that these revelations have dealt a further blow to the credibility and effectiveness of the essential legal tool to lawfully transfer personal data from EU countries to U.S.: the so called Safe Harbour[1] scheme.

The Safe Harbour is the result of the EU decision 520/2000/EC[2] according to Articles 25 and 26 of the data protection Directive 95/46/EC, setting forth the legal framework for transfers of personal data from the EU to third countries outside the EEA.

The current Safe Harbour decision 520/2000/EC allows free transfer of personal data from EU Member States to companies in the U.S. which voluntarily sign up and adhere to the Safe Harbour Principles[3].

From a commercial point of view the Safe Harbour scheme should represent the essential lawful pillar for the services provided in the EU by companies established in U.S.: in 2013 the Safe Harbor list includes more than 3000 U.S. companies.

Considering the paramount changes in all sectors brought by the global and digital economy in the last years, the functioning of the Safe Harbour has to face a complex risk figure in terms of:

- exponential increase in data flows which used to be ancillary but are now central to the rapid growth of the digital economy and the very significant developments in data collection, processing and use
- critical importance of data flows notably for the transatlantic economy
- recent information on U.S. mass surveillance programs based on the data collected by the U.S. companies offering services to the EU companies and EU citizens

The news – EU Commission reviews and actions plan

Thus the European Commission has recently reviewed the functioning of the Safe Harbour scheme within the context of a number of existing agreements with U.S. concerning the use of EU citizens data, such as the Passenger Name Records (PNR) and the Terrorist Finance Tracking Programme (TFTP).

Commission reports and communications to the European Parliament are available with the press release of November 27 at : http://europa.eu/rapid/press-release_IP-13-1166_en.htm

and include:

- Communication: 'Rebuilding Trust in EU-U.S. Data Flows';
- Communication: on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU';

1 http://export.gov/safeharbor/eu/eg_main_018475.asp

2 Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related FAQs issued by the US Department of Commerce in OJ 215 of 28 August 2000

3 The financial services and telecommunication industries are outside the U.S. Federal Trade Commission enforcement powers and therefore excluded from the Safe Harbour

- Report on the findings of the EU-U.S. Working Group;
- Review of the existing agreements on Passenger Name Records and the Terrorist Finance Tracking Program.

A number of critical issues has been underlined by the Commission review as well as by the considerations and in some cases also actions by some EU Data protection Authorities[4].

The Commission reports that *"due to deficiencies in transparency and enforcement of the arrangement, specific problems still persist and should be addressed:*

a) transparency of privacy policies of Safe Harbour members,

b) effective application of Privacy Principles by companies in the US, and

c) effectiveness of the enforcement.

Furthermore, the large scale access by intelligence agencies to data transferred to the US by Safe Harbour certified companies raises additional serious questions regarding the continuity of data protection rights of Europeans when their data in transferred to the US."

Six main actions have been identified by the European Commission:

1. *"Adoption of the EU's draft Data Protection Regulation by Spring 2013;*
2. *Improvement of the functioning of the Safe Harbour scheme (which provides a legal basis for the transfers of personal data from the EU to companies in the U.S. for commercial purposes);*
3. *Swift conclusion of the current negotiations on the "umbrella agreement" for transfers and processing of data in the context of police and judicial co-operation;*
4. *Use by the U.S. administration of the existing Mutual Legal Assistance and Sectoral agreements, whenever transfers of data are required for law enforcement purposes;*
5. *Extension of the legal safeguards available to U.S. citizens to EU citizens, not resident in the U.S; and*
6. *Accession by the U.S. to the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (as it acceded to the 2001 Convention on Cybercrime)."*

Specifically for the Safe Harbour scheme, the European Commission makes 13 recommendations to improve the functioning and requires the U.S. authorities to identify remedies by summer 2014. The Commission will then review the functioning of the Safe Harbour scheme based on the implementation of these 13 recommendations.

"The 13 Recommendations are:

Transparency

1. *Self-certified companies should publicly disclose their privacy policies.*
2. *Privacy policies of self-certified companies' websites should always include a link to the Department of Commerce Safe Harbour website which lists all the 'current' members of the scheme.*
3. *Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services.*
4. *Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.*

Redress

5. *The privacy policies on companies' websites should include a link to the alternative dispute resolution (ADR) provider.*
6. *ADR should be readily available and affordable.*
7. *The Department of Commerce should monitor more systematically ADR providers regarding the*

4 German data protection commissioners have decided not to issue new permissions for data transfers to non-EU countries (for example for the use of certain cloud services). They will also examine whether data transfers on the basis of the Safe Harbour should be suspended.

transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.

Enforcement

8. *Following the certification or recertification of companies under Safe Harbour, a certain percentage of these companies should be subject to ex officio investigations of effective compliance of their privacy policies (going beyond control of compliance with formal requirements).*
9. *Whenever there has been a finding of non-compliance, following a complaint or an investigation, the company should be subject to follow-up specific investigation after 1 year.*
10. *In case of doubts about a company's compliance or pending complaints, the Department of Commerce should inform the competent EU data protection authority.*
11. *False claims of Safe Harbour adherence should continue to be investigated*

Access by US authorities

12. *Privacy policies of self-certified companies should include information on the extent to which US law allows public authorities to collect and process data transferred under the Safe Harbour. In particular companies should be encouraged to indicate in their privacy policies when they apply exceptions to the Principles to meet national security, public interest or law enforcement requirements.*
13. *It is important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary or proportionate."*

Some comments

The type of findings identified by the review and the complexity and quantity of the recommendations resulting for the Safe Harbour scheme, appear to be very challenging and require strong common EU &U.S. commitment to reach practical and satisfactory solutions considering, first of all and at the utmost level, the respect of the EU fundamental rights[5] of the individuals.

Furthermore, the consequences of inappropriate or worse, unilateral choices, could impact the expectations of the companies that lawfully provide their services as well as the availability of effective information society services with efficient and lower-cost solutions for individuals and businesses.

Specifically for the cloud services, backbone of many online services and largely driven by U.S. companies, uncertainty on the effective coverage provided by the Safe Harbour scheme could lead to inappropriate allocation of responsibilities, always bearing in mind the rights of individuals and the respect of the EU data protection & privacy legislation.

In fact, possible alternatives to the Safe Harbor scheme such as the standard contractual clauses pursuant to EU directive 2010/87/EU or the adoption of Binding Corporate Rules pursuant to article 26 of EU directive 95/46/EC, imply more complexity in the contractual agreements considering the high number of dynamic and multilayered service providers involved in a cloud service, but mostly represent an unfair shift of responsibility from the concerned regulatory authorities toward the U.S.-EU business community. In this sense a specific Cloud Computing EU regulation, bearing in mind that the legislative process of the new EU privacy regulation appears complex and perhaps long-term duration, could represent a short term necessity.

5 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF