COUNCIL OF
THE EUROPEAN UNION

Brussels, 29 November 2013

17067/13

JAI 1095
USA 64
DATAPROTECT 190
COTER 154

COVER NOTE
from: Secretary-General of the European Commission,
signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt: 28 November 2013
to: Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.: COM(2013) 846 final
Subject: Communication from the Commission to the European Parliament and the Council
Rebuilding Trust in EU-US Data Flows


Encl.: COM(2013) 846 final
COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Rebuilding Trust in EU-US Data Flows
1. INTRODUCTION: THE CHANGING ENVIRONMENT OF EU-US DATA PROCESSING

The European Union and the United States are strategic partners, and this partnership is critical for the promotion of our shared values, our security and our common leadership in global affairs.

However, trust in the partnership has been negatively affected and needs to be restored. The EU, its Member States and European citizens have expressed deep concerns at revelations of large-scale US intelligence collection programmes, in particular as regards the protection of personal data1. Mass surveillance of private communication, be it of citizens, enterprises or political leaders, is unacceptable.

Transfers of personal data are an important and necessary element of the transatlantic relationship. They form an integral part of commercial exchanges across the Atlantic including for new growing digital businesses, such as social media or cloud computing, with large amounts of data going from the EU to the US. They also constitute a crucial component of EU-US co-operation in the law enforcement field, and of the cooperation between Member States and the US in the field of national security. In order to facilitate data flows, while ensuring a high level of data protection as required under EU law, the US and the EU have put in place a series of agreements and arrangements.

Commercial exchanges are addressed by Decision 2000/520/EC2 (hereafter “the Safe Harbour Decision”). This Decision provides a legal basis for transfers of personal data from the EU to companies established in the US which have adhered to the Safe Harbour Privacy Principles. Exchange of personal data between the EU and the US for the purposes of law enforcement, including the prevention and combating of terrorism and other forms of serious crime, is governed by a number of agreements at EU level. These are the Mutual Legal Assistance Agreement3, the Agreement on the use and transfer of Passenger Name Records (PNR)4, the Agreement on the processing and transfer of Financial Messaging Data for the purpose of the Terrorist Finance Tracking Program (TFTP)5, and the Agreement between Europol and the US. These Agreements respond to important security challenges and meet the common security interests of the EU and US, whilst providing a high level of protection of personal data. In addition, the EU and the US are currently negotiating a framework agreement on data protection in the field of police and judicial cooperation (“umbrella agreement”)6. The aim is to ensure a high level of data protection for citizens whose data is exchanged thereby further

---

1 For the purposes of this Communication, references to EU citizens include also non-EU data subjects which fall within the scope of European Union’s data protection law.


advancing EU-US cooperation in the combating of crime and terrorism on the basis of shared values and agreed safeguards. These instruments operate in an environment in which personal data flows are acquiring increasing relevance.

On the one hand, the development of the digital economy has led to exponential growth in the quantity, quality, diversity and nature of data processing activities. The use of electronic communication services by citizens in their daily lives has increased. Personal data has become a highly valuable asset: the estimated value of EU citizens' data was €315bn in 2011 and has the potential to grow to nearly €1tn annually by 2020. The market for the analysis of large sets of data is growing by 40% per year worldwide. Similarly, technological developments, for example related to cloud computing, put into perspective the notion of international data transfer as cross-border data flows are becoming a day to day reality. The increase in the use of electronic communications and data processing services, including cloud computing, has also substantially expanded the scope and significance of transatlantic data transfers. Elements such as the central position of US companies in the digital economy, the transatlantic routing of a large part of electronic communications and the volume of electronic data flows between the EU and the US have become even more relevant. On the other hand, modern methods of personal data processing raise new and important questions. This applies both to new means of large-scale processing of consumer data by private companies for commercial purposes, and to the increased ability of large-scale surveillance of communications data by intelligence agencies. Large-scale US intelligence collection programmes, such as PRISM affect the fundamental rights of Europeans and, specifically, their right to privacy and to the protection of personal data. These programmes also point to a connection between Government surveillance and the processing of data by private companies, notably by US internet companies. As a result, they may therefore have an economic impact. If citizens are concerned about the large-scale processing of their personal data by private companies or by the surveillance of their data by intelligence agencies when using Internet services, this may affect their trust in the digital economy, with potential negative consequences on growth. These developments expose EU-US data flows to new challenges. This Communication addresses these challenges. It explores the way forward on the basis of the findings contained in the Report of the EU Co-Chairs of the ad hoc EU-US Working Group and the Communication on the Safe Harbour. It seeks to provide an effective way forward to rebuild trust and reinforce EU-US cooperation in these fields and strengthen the broader transatlantic relationship.

This Communication is based on the premise that the standard of protection of personal data must be addressed in its proper context, without affecting other dimensions of EU-US relations, including the on-going negotiations for a Transatlantic Trade and Investment Partnership. For this reason, data protection standards will not be negotiated within the Transatlantic Trade and Investment Partnership, which will fully respect the data protection rules.

---

[10] For example, the combined number of unique visitors to Microsoft Hotmail, Google Gmail and Yahoo! Mail from European countries in June 2012 totalled over 227 million, eclipsing that of all other providers. The combined number of unique European users accessing Facebook and Facebook Mobile in March 2012 was 196.5 million, making Facebook the largest social network in Europe. Google is the leading internet search engine with 90.2% of worldwide internet users. US mobile messaging service What’s App was used by 91% of iPhone users in Germany in June 2013.
It is important to note that whilst the EU can take action in areas of EU competence, in particular to safeguard the application of EU law\(^{11}\), national security remains the sole responsibility of each Member State\(^{12}\).

2. **THE IMPACT ON THE INSTRUMENTS FOR DATA TRANSFERS**

First, as regards data transferred for commercial purposes, the Safe Harbour has proven to be an important vehicle for EU-US data transfers. Its commercial importance has grown as personal data flows have taken on greater prominence in the transatlantic commercial relationship. Over the past 13 years, the Safe Harbour scheme has evolved to include more than 3,000 companies, over half of which have signed up within the last five years. Yet concerns about the level of protection of personal data of EU citizens transferred to the US under the Safe Harbour scheme have grown. The voluntary and declaratory nature of the scheme has sharpened focus on its transparency and enforcement. While a majority of US companies apply its principles, some self-certified companies do not. The non-compliance of some self-certified companies with the Safe Harbour Privacy Principles places such companies at a competitive advantage in relation to European companies operating in the same markets.

Moreover, while under the Safe Harbour, limitations to data protection rules are permitted where necessary on grounds of national security\(^{13}\), the question has arisen whether the large-scale collection and processing of personal information under US surveillance programmes is necessary and proportionate to meet the interests of national security. It is also clear from the findings of the ad hoc EU-US Working Group that, under these programmes, EU citizens do not enjoy the same rights and procedural safeguards as Americans.

The reach of these surveillance programmes, combined with the unequal treatment of EU citizens, brings into question the level of protection afforded by the Safe Harbour arrangement. The personal data of EU citizens sent to the US under the Safe Harbour may be accessed and further processed by US authorities in a way incompatible with the grounds on which the data was originally collected in the EU and the purposes for which it was transferred to the US. A majority of the US internet companies that appear to be more directly concerned by these programmes are certified under the Safe Harbour scheme.

Second, as regards exchanges of data for law enforcement purposes, the existing Agreements (PNR, TFTP) have proven highly valuable tools to address common security threats linked to serious transnational crime and terrorism, whilst laying down safeguards that ensure a high level of data protection\(^{14}\). These safeguards extend to EU citizens, and the Agreements provide for mechanisms to review their implementation and to address issues of concern related thereto. The TFTP Agreement also establishes a system of oversight, with EU independent overseers checking how data covered by the Agreement is searched by the US.

Against the backdrop of concerns raised in the EU about US surveillance programmes, the European Commission has used those mechanisms to check how the agreements are applied. In the case of the PNR Agreement, a joint review was conducted, involving data protection

---

\(^{11}\) See Judgment of the Court of Justice of the European Union in Case C-300/11, ZZ v Secretary of State for the Home Department.

\(^{12}\) Article 4(2) TEU.

\(^{13}\) See e.g. Safe Harbour Decision, Annex I.

\(^{14}\) See Joint Report from the Commission and the U.S. Treasury Department regarding the value of TFTP Provided Data pursuant to Article 6 (6) of the Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program.
experts from the EU and the US, looking at how the Agreement has been implemented\textsuperscript{15}. That review did not give any indication that US surveillance programmes extend to or have impact on the passenger data covered by the PNR Agreement. In the case of the TFTP Agreement, the Commission opened formal consultations after allegations were made of US intelligence agencies directly accessing personal data in the EU, contrary to the Agreement. These consultations did not reveal any elements proving a breach of the TFTP Agreement, and they led the US to provide written assurance that no direct data collection has taken place contrary to the provisions of the Agreement.

The large-scale collection and processing of personal information under US surveillance programmes call, however, for a continuation of very close monitoring of the implementation of the PNR and TFTP Agreements in the future. The EU and the US have therefore agreed to advance the next Joint Review of the TFTP Agreement, which will be held in Spring 2014. Within that and future joint reviews, greater transparency will be ensured on how the system of oversight operates and on how it protects the data of EU citizens. In parallel, steps will be taken to ensure that the system of oversight continues to pay close attention to how data transferred to the US under the Agreement is processed, with a focus on how such data is shared between US authorities.

Third, the increase in the volume of processing of personal data underlines the importance of the legal and administrative safeguards that apply. One of the goals of the Ad Hoc EU-US Working Group was to establish what safeguards apply to minimise the impact of the processing on the fundamental rights of EU citizens. Safeguards are also necessary to protect companies. Certain US laws such as the Patriot Act, enable US authorities to directly request companies access to data stored in the EU. Therefore, European companies, and US companies present in the EU, may be required to transfer data to the US in breach of EU and Member States’ laws, and are consequently caught between conflicting legal obligations.

Legal uncertainty deriving from such direct requests may hold back the development of new digital services, such as cloud computing, which can provide efficient, lower-cost solutions for individuals and businesses.

3. **Ensuring the effectiveness of data protection**

Transfers of personal data between the EU and the US are an essential component of the transatlantic commercial relationship. Information sharing is also an essential component of EU-US security cooperation, critically important to the common goal of preventing and combating serious crime and terrorism. However, recent revelations about US intelligence collection programmes have negatively affected the trust on which this cooperation is based. In particular, it has affected trust in the way personal data is processed. The following steps should be taken to restore trust in data transfers for the benefit of the digital economy, security both in the EU and in the US, and the broader transatlantic relationship.

3.1. **The EU data protection reform**

The data protection reform proposed by the Commission in January 2012\textsuperscript{16} provides a key response as regards the protection of personal data. Five components of the proposed Data Protection package are of particular importance.

\textsuperscript{15} See on the Commission report “Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security”.

First, as regards territorial scope, the proposed regulation makes clear that companies that are not established in the Union will have to apply EU data protection law when they offer goods and services to European consumers or monitor their behaviour. In other words, the fundamental right to data protection will be respected, independently of the geographical location of a company or of its processing facility.

Secondly, on international transfers, the proposed regulation establishes the conditions under which data can be transferred outside the EU. Transfers can only be allowed where these conditions, which safeguard the individuals' rights to a high level of protection, are met.

Thirdly, concerning enforcement, the proposed rules provide for proportionate and dissuasive sanctions (up to 2% of a company's annual global turnover) to make sure that companies comply with EU law. The existence of credible sanctions will increase companies' incentive to comply with EU law.

Fourthly, the proposed regulation includes clear rules on the obligations and liabilities of data processors such as cloud providers, including on security. As the revelations about US intelligence collection programmes have shown, this is critical because these programmes affect data stored in the cloud. Also, companies providing storage space in the cloud which are asked to provide personal data to foreign authorities will not be able to escape their responsibility by reference to their status as data processors rather than data controllers.

Fifth, the package will lead to the establishment of comprehensive rules for the protection of personal data processed in the law enforcement sector.

It is expected that the package will be agreed upon in a timely manner in the course of 2014.

3.2. Making Safe Harbour safer

The Safe Harbour scheme is an important component of the EU-US commercial relationship, relied upon by companies on both sides of the Atlantic.

The Commission’s report on the functioning of Safe Harbour has identified a number of weaknesses in the scheme. As a result of a lack of transparency and of enforcement, some self-certified Safe Harbour members do not, in practice, comply with its principles. This has a negative impact on EU citizens’ fundamental rights. It also creates a disadvantage for European companies compared to those competing US companies that are operating under the scheme but in practice not applying its principles. This weakness also affects the majority of US companies which properly apply the scheme. Safe Harbour also acts as a conduit for the

with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

The Commission takes note that the European Parliament confirmed and strengthened this important principle, enshrined in Art. 3 of the proposed Regulation, in its vote of 21 October 2013 on the data protection reform reports of MEPs Jan-Philipp Albrecht and Dimitrios Droutsas in the Committee for Civil Liberties, Justice and Home Affairs (LIBE).

The Commission takes note that in its vote of 21 October 2013, the LIBE Committee of the European Parliament proposed to include a provision in the future Regulation that would subject requests from foreign authorities to access personal data collected in the EU to the obtaining of a prior authorisation from a national data protection authority, where such a request would be issued outside a mutual legal assistance treaty or another international agreement.

The Commission takes note that in its vote of 21 October 2013, the LIBE Committee proposed strengthening the Commission’s proposal by providing that fines can go up to 5% of the annual worldwide turnover of a company.

The Commission takes note that in its vote of 21 October 2013, the LIBE Committee endorsed the strengthening of the obligations and liabilities of data processors, in the particular with regard to Art. 26 of the proposed Regulation.

The Conclusions of the October 2013 European Council state that: "It is important to foster the trust of citizens and businesses in the digital economy. The timely adoption of a strong EU General Data Protection framework and the Cyber-security Directive is essential for the completion of the Digital Single Market by 2015".
transfer of the personal data of EU citizens from the EU to the US by companies required to surrender data to US intelligence agencies under the US intelligence collection programmes. Unless the deficiencies are corrected, it therefore constitutes a competitive disadvantage for EU business and has a negative impact on the fundamental right to data protection of EU citizens.

The shortcomings of the Safe Harbour scheme have been underlined by the response of European Data Protection Authorities to the recent surveillance revelations. Article 3 of the Safe Harbour Decision authorises these authorities to suspend, under certain conditions, data flows to certified companies. 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. The risk is that such measures, taken at national level, would create differences in coverage, which means that Safe Harbour would cease to be a core mechanism for the transfer of personal data between the EU and the US.

The Commission has the authority under Directive 95/46/EC to suspend or revoke the Safe Harbour decision if the scheme no longer provides an adequate level of protection. Furthermore, Article 3 of the Safe Harbour Decision provides that the Commission may reverse, suspend or limit the scope of the decision, while, under article 4, it may adapt the decision at any time in the light of experience with its implementation.

Against this background, a number of policy options can be considered, including:

- Maintaining the status quo;
- Strengthening the Safe Harbour scheme and reviewing its functioning thoroughly;
- Suspending or revoking the Safe Harbour decision.

Given the weaknesses identified, the current implementation of Safe Harbour cannot be maintained. However, its revocation would adversely affect the interests of member companies in the EU and in the US. The Commission considers that Safe Harbour should rather be strengthened.

The improvements should address both the structural shortcomings related to transparency and enforcement, the substantive Safe Harbour principles and the operation of the national security exception.

More specifically, for Safe Harbour to work as intended, the monitoring and supervision by US authorities of the compliance of certified companies with the Safe Harbour Privacy Principles needs to be more effective and systematic. The transparency of certified companies' privacy policies needs to be improved. The availability and affordability of dispute resolution mechanisms also needs to be ensured to EU citizens.

As a matter of urgency, the Commission will engage with the US authorities to discuss the shortcomings identified. Remedies should be identified by summer 2014 and implemented as soon as possible. On the basis thereof, the Commission will undertake a complete stock taking of the functioning of the Safe Harbour. This broader review process should involve open consultation and a debate in the European Parliament and the Council as well as discussions with the US authorities.

22 Specifically, pursuant to Art. 3 of the Safe Harbour Decision, such suspensions may take place in cases where there is a substantial likelihood that the Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the organisation with notice and an opportunity to respond.

It is also important that the national security exception foreseen by the Safe Harbour Decision, is used only to an extent that is strictly necessary and proportionate.

3.3. Strengthening data protection safeguards in law enforcement cooperation

The EU and the US are currently negotiating a data protection “umbrella” agreement on transfers and processing of personal information in the context of police and judicial cooperation in criminal matters. The conclusion of such an agreement providing for a high level of protection of personal data would represent a major contribution to strengthening trust across the Atlantic. By advancing the protection of EU data citizens’ rights, it would help strengthen transatlantic cooperation aimed at preventing and combating crime and terrorism.

According to the decision authorising the Commission to negotiate the umbrella agreement, the aim of the negotiations should be to ensure a high level of protection in line with the EU data protection acquis. This should be reflected in agreed rules and safeguards on, inter alia, purpose limitation, the conditions and the duration of the retention of data. In the context of the negotiation, the Commission should also obtain commitments on enforceable rights including judicial redress mechanisms for EU citizens not resident in the US. Close EU-US cooperation to address common security challenges should be mirrored by efforts to ensure that citizens benefit from the same rights when the same data is processed for the same purposes on both sides of the Atlantic. It is also important that derogations based on national security needs are narrowly defined. Safeguards and limitations should be agreed in this respect.

These negotiations provide an opportunity to clarify that personal data held by private companies and located in the EU will not be directly accessed by or transferred to US law enforcement authorities outside of formal channels of co-operation, such as Mutual Legal Assistance agreements or sectoral EU-US Agreements authorising such transfers. Access by other means should be excluded, unless it takes place in clearly defined, exceptional and judicially reviewable situations. The US should undertake commitments in that regard.

An "umbrella agreement" agreed along those lines, should provide the general framework to ensure a high level of protection of personal data when transferred to the US for the purpose of preventing or combating crime and terrorism. Sectoral agreements should, where necessary due to the nature of the data transfer concerned, lay down additional rules and safeguards, building on the example of the EU-US PNR and TFTP Agreements, which set strict conditions for transfer of data and safeguards for EU citizens.

---

24 See the relevant passage of the Joint Press Statement following the EU-US-Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We are therefore, as a matter of urgency, committed to advancing rapidly in the negotiations on a meaningful and comprehensive data protection umbrella agreement in the field of law enforcement. The agreement would act as a basis to facilitate transfers of data in the context of police and judicial cooperation in criminal matters by ensuring a high level of personal data protection for U.S. and EU citizens. We are committed to working to resolve the remaining issues raised by both sides, including judicial redress (a critical issue for the EU). Our aim is to complete the negotiations on the agreement ahead of summer 2014."

25 See the relevant passage of the Joint Press Statement following the EU-US Justice and Home Affairs Ministerial Meeting of 18 November 2013 in Washington: "We also underline the value of the EU-U.S. Mutual Legal Assistance Agreement. We reiterate our commitment to ensure that it is used broadly and effectively for evidence purposes in criminal proceedings. There were also discussions on the need to clarify that personal data held by private entities in the territory of the other party will not be accessed by law enforcement agencies outside of legally authorized channels. We also agree to review the functioning of the Mutual Legal Assistance Agreement, as contemplated in the Agreement, and to consult each other whenever needed."
3.4. Addressing European concerns in the on-going US reform process

US President Obama has announced a review of US national security authorities’ activities, including of the applicable legal framework. This on-going process provides an important opportunity to address EU concerns raised by recent revelations about US intelligence collection programmes. The most important changes would be extending the safeguards available to US citizens and residents to EU citizens not resident in the US, increased transparency of intelligence activities, and further strengthening oversight. Such changes would restore trust in EU-US data exchanges, and promote the use of Internet services by Europeans.

With respect to extending the safeguards available to US citizens and residents to EU citizens, legal standards in relation to US surveillance programmes which treat US and EU citizens differently should be reviewed, including from the perspective of necessity and proportionality, keeping in mind the close transatlantic security partnership based on common values, rights and freedoms. This would reduce the extent to which Europeans are affected by US intelligence collection programmes.

More transparency is needed on the legal framework of US intelligence collection programmes and its interpretation by US Courts as well as on the quantitative dimension of US intelligence collection programmes. EU citizens would also benefit from such changes. The oversight of US intelligence collection programmes would be improved by strengthening the role of the Foreign Intelligence Surveillance Court and by introducing remedies for individuals. These mechanisms could reduce the processing of personal data of Europeans that are not relevant for national security purposes.

3.5. Promoting privacy standards internationally

Issues raised by modern methods of data protection are not limited to data transfer between the EU and the US. A high level of protection of personal data should also be guaranteed to any individual. EU rules on collection, processing and transfer of data should be promoted internationally.

Recently, a number of initiatives have been proposed to promote the protection of privacy, particularly on the internet. The EU should ensure that such initiatives, if pursued, fully take into account the principles of protecting fundamental rights, freedom of expression, personal data and privacy as set out in EU law and in the EU Cyber Security Strategy, and do not undermine the freedom, openness and security of cyber space. This includes a democratic and efficient multi stakeholder governance model.

The on-going reforms of data protection laws on both sides of the Atlantic also provide the EU and the US a unique opportunity to set the standard internationally. Data exchanges across the Atlantic and beyond would greatly benefit from the strengthening of the US domestic legal framework, including the passage of the "Consumer Privacy Bill of Rights" announced by President Obama in February 2012 as part of a comprehensive blueprint to improve consumers’ privacy protections. The existence of a set of strong and enforceable data protection rules enshrined in both the EU and the US would constitute a solid basis for cross-border data flows.

In view of promoting privacy standards internationally, accession to the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (“Convention 108”), which is open to countries which are not member of the Council of Europe, should also be favoured. Safeguards and guarantees agreed in international fora should result in a high level of protection compatible with what is required under EU law.

26 See in this respect the draft resolution proposed to the UN General Assembly by Germany and Brazil – calling for the protection of privacy online as offline.

27 The US is already party to another Council of Europe convention: the 2001 Convention on Cybercrime (also known as the "Budapest Convention").
4. CONCLUSIONS AND RECOMMENDATIONS

The issues identified in this Communication require action to be taken by the US as well as by the EU and its Member States.

The concerns around transatlantic data exchanges are, first of all, a wake-up call for the EU and its Member States to advance swiftly and with ambition on the data protection reform. It shows that a strong legislative framework with clear rules that are enforceable also in situations when data are transferred abroad is, more than ever, a necessity. The EU institutions should therefore continue working towards the adoption of the EU data protection reform by spring 2014, to make sure that personal data is effectively and comprehensively protected.

Given the significance of transatlantic data flows, it is essential that the instruments on which these exchanges are based appropriately address the challenges and opportunities of the digital era and new technological developments like cloud computing. Existing and future arrangements and agreements should ensure that the continuity of a high level of protection is guaranteed over the Atlantic.

A robust Safe Harbour scheme is in the interests of EU and US citizens and companies. It should be strengthened by better monitoring and implementation in the short term, and, on this basis, by a broader review of its functioning. Improvements are necessary to ensure that the original objectives of the Safe Harbour Decision – i.e. continuity of data protection, legal certainty and free EU-US flow of data – are still met. These improvements should focus on the need for the US authorities to better supervise and monitor the compliance of self-certified companies with the Safe Harbour Privacy Principles.

It is also important that the national security exception foreseen by the Safe Harbour Decision is used only to an extent that is strictly necessary and proportionate.

In the area of law enforcement, the current negotiations of an “umbrella agreement” should result in a high level of protection for citizens on both sides of the Atlantic. Such an agreement would strengthen the trust of Europeans in EU-US data exchanges, and provide a basis to further develop EU-US security cooperation and partnership. In the context of the negotiation, commitments should be secured to the effect that procedural safeguards, including judicial redress, are available to Europeans who are not resident in the US.

Commitments should be sought from the US administration to ensure that personal data held by private entities in the EU will not be accessed directly by US law enforcement agencies outside of formal channels of co-operation, such as Mutual Legal Assistance agreements and sectoral EU-US Agreements such as PNR and TFTP authorising such transfers under strict conditions, except in clearly defined, exceptional and judicially reviewable situations.

The US should also extend the safeguards available to US citizens and residents to EU citizens not resident in the US, ensure the necessity and proportionality of the programmes, greater transparency and oversight in the legal framework applicable to US national security authorities.

Areas listed in this communication will require constructive engagement from both sides of the Atlantic. Together, as strategic partners, the EU and the US have the ability to overcome the current tensions in the transatlantic relationship and rebuild trust in EU-US data flows. Undertaking joint political and legal commitments on further cooperation in these areas will strengthen the overall transatlantic relationship.
Brussels, 29 November 2013

17069/13

DATAPROTECT 191
USA 65
JAI 1097

COVER NOTE
from: Secretary-General of the European Commission,
signed by Mr Jordi AYET PUIGARNAU, Director
date of receipt: 28 November 2013
to: Mr Uwe CORSEPIUS, Secretary-General of the Council of the European Union
No Cion doc.: COM(2013) 847 final
Subject: Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU


Encl.: COM(2013) 847 final
COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU
COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU

1. INTRODUCTION

Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter “data protection Directive”) sets the rules for transfers of personal data from EU Member States to other countries outside the EU\(^1\) to the extent such transfers fall within the scope of this instrument\(^2\).

Under the Directive, the Commission may find that a third country ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into in order to protect rights of individuals in which case the specific limitations on data transfers to such a country would not apply. These decisions are commonly referred to as "adequacy decisions".

On 26 July 2000, the Commission adopted Decision 520/2000/EC\(^3\) (hereafter “Safe Harbour decision”) recognising the Safe Harbour Privacy Principles and Frequently Asked Questions (respectively “the Principles” and “FAQs”), issued by the Department of Commerce of the United States, as providing adequate protection for the purposes of personal data transfers from the EU. The Safe Harbour decision was taken following an opinion of the Article 29 Working Party and an opinion of the Article 31 Committee delivered by a qualified majority of Member States. In accordance with Council Decision 1999/468 the Safe Harbour Decision was subject to prior scrutiny by the European Parliament.

As a result, the current Safe Harbour decision allows free transfer\(^4\) of personal information from EU Member States\(^5\) to companies in the US which have signed up to the Principles in circumstances where the transfer would otherwise not meet the EU standards for adequate level of data protection given the substantial differences in privacy regimes between the two sides of Atlantic.

The functioning of the current Safe Harbour arrangement relies on commitments and self-certification of adhering companies. Signing up to these arrangements is voluntary, but the rules are binding for those who sign up. The fundamental principles of such an arrangement are:

a) Transparency of adhering companies' privacy policies,

b) Incorporation of the Safe Harbour principles in companies' privacy policies, and

---

\(^1\) Articles 25 and 26 of the data protection Directive set forth the legal framework for transfers of personal data from the EU to third countries outside the EEA.

\(^2\) Additional rules have been laid down in Article 13 of Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters to the extent such transfers concern personal data transmitted or made available by one Member State to another Member State, who subsequently intends to transfer those data to a third state or international body for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal sanctions.


\(^4\) The above does not exclude the application to the data processing of other requirements that may exist under national legislation implementing the EU data protection directive.

c) Enforcement, including by public authorities.

This fundamental basis of the Safe Harbour has to be reviewed in the new context of:

a) the 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,

b) the critical importance of data flows notably for the transatlantic economy,\(^6\)

c) the rapid growth of the number of companies in the US adhering to the Safe Harbour scheme which has increased by eight-fold since 2004 (from 400 in 2004 to 3,246 in 2013),

d) the information recently released on US surveillance programmes which raises new questions on the level of the protection the Safe Harbour arrangement is deemed to guarantee.

Against this background, this Communication takes stock of the functioning of the Safe Harbour scheme. It is based on evidence gathered by the Commission, the work of the EU-US Privacy Contact Group in 2009, a Study prepared by an independent contractor in 2008\(^7\) and information received in the ad hoc EU-US Working Group (the “Working Group”) established following the revelations on US surveillance programmes (see a parallel Document). This Communication follows the two Commission Assessment Reports in the start-up period of the Safe Harbour arrangement, respectively in 2002\(^8\) and 2004\(^9\).

2. Structure and Functioning of Safe Harbour

2.1. Structure of the Safe Harbour

A US company that wants to adhere to the Safe Harbour must: (a) identify in its publicly available privacy policy that it adheres to the Principles and actually does comply with the Principles, as well as (b) self-certify i.e., declare to the US Department of Commerce that it is in compliance with the Principles. The self-certification must be resubmitted on an annual basis. The Safe Harbour Privacy Principles attached in Annex I to the Safe Harbour Decision include requirements on both the substantive protection of personal data (data integrity, security, choice, and onward transfer principles) and the procedural rights of data subjects (notice, access, and enforcement principles).

As to the enforcement of the Safe Harbour scheme in the US, two US institutions play a major role: the US Department of Commerce and the US Federal Trade Commission.

The Department of Commerce reviews every Safe Harbour self-certification and every annual recertification submission that it receives from companies to ensure that they include

---

\(^6\) According to some studies, if services and cross-border data flows were to be disrupted as a consequence of discontinuity of binding corporate rules, model contract clauses and the Safe Harbour, the negative impact on EU GDP could reach -0.8% to -1.3% and EU services exports to the US would drop by -6.7% due to loss of competitiveness. See: “The Economic Importance of Getting Data Protection Right”, a study by the European Centre for International Political Economy for the US Chamber of Commerce, March 2013.

\(^7\) Impact Assessment Study prepared for the European Commission in 2008 by the Centre de Recherche Informatique et Droit (CRID) of the University of Namur.


all the elements required to be a member of the scheme. It updates a list of companies which have filed self-certification letters and publishes the list and letters on its website. Furthermore, it monitors the functioning of Safe Harbour and removes from the list companies not complying with the Principles.

The Federal Trade Commission, within its powers in the field of consumer protection, intervenes against unfair or deceptive practices pursuant to Section 5 of the Free Trade Commission Act. The Federal Trade Commission's enforcement actions include inquiries on false statements of adherence to Safe Harbour and non-compliance with these Principles by companies which are members of the scheme. In the specific cases of enforcing the Safe Harbour Principles against air carriers, the competent body is the US Department of Transportation.

The current Safe Harbour Decision is part of EU law which has to be applied by Member State Authorities. Under the Decision, the EU national data protection authorities (DPAs) have the right to suspend data transfers to Safe Harbour certified companies in specific cases. The Commission is not aware of any cases of suspension by a national data protection authority since the establishment of Safe Harbour in 2000. Independently of the powers they enjoy under the Safe Harbour Decision, EU national data protection authorities are competent to intervene, including in the case of international transfers, in order to ensure compliance with the general principles of data protection set forth in the 1995 Data Protection Directive.

As recalled in the current Safe Harbour Decision, it is the competence of the Commission – acting in accordance with the examination procedure set out in Regulation 182/2011 – to adapt the Decision, to suspend it or limit its scope at any time, in the light of experience with its implementation. This is notably foreseen if there is a systemic failure on the US side, for example if a body responsible for ensuring compliance with the Safe Harbour Privacy Principles in the United States is not effectively fulfilling its role, or if the level of protection provided by the Safe Harbour Principles is overtaken by the requirements of US legislation. As with any other Commission decision, it can also be amended for other reasons or even revoked.

2.2. The functioning of the Safe Harbour

The 3246 certified companies include both small and big companies. While financial services and telecommunication industries are outside the Federal Trade Commission enforcement powers and therefore excluded from the Safe Harbour, many industry and services sectors are present among certified companies, including well known Internet companies and industries ranging from information and computer services to pharmaceuticals, travel and tourism services, healthcare or credit card services. These are mainly US companies that provide services in the EU internal market. There are also subsidiaries of some

---

10 If a company’s certification or recertification fails to meet Safe Harbour requirements, the Department of Commerce notifies the company requesting steps to be taken (e.g., clarifications, changes in policy description) before the company’s certification may be finalised.

11 Under Title 49 of the US Code Section 41712.

12 More specifically, suspension of transfers can be required in two situations, where:
   (a) the government body in the US has determined that the company is violating the Safe Harbour Privacy Principles; or
   (b) there is a substantial likelihood that the Safe Harbour Privacy Principles are being violated; there is a reasonable basis for believing that the enforcement mechanism concerned is not taking or will not take adequate and timely steps to settle the case at issue; the continuing transfer would create an imminent risk of grave harm to data subjects; and the competent authorities in the Member State have made reasonable efforts under the circumstances to provide the company with notice and an opportunity to respond.

13 On 26 September 2013 the number of Safe Harbour organizations listed as “current” on the Safe Harbour List was 3246, as “not current” 935.

14 Safe Harbour organizations with 250 or less employees: 60% (1925 of 3246). Safe Harbour organizations with 251 or more employees: 40% (1295 of 3246).

15 For example MasterCard deals with thousands of banks and the company is a clear example of a case where Safe Harbour cannot be replaced by other legal instruments for personal data transfers such as binding corporate rules or contractual arrangements.
EU firms such as Nokia or Bayer. 51% are firms that process data of employees in Europe transferred to the US for human resource purposes\(^{16}\).

There has been a **growing concern** among some data protection authorities in the EU about data transfers under the current Safe Harbour scheme. Some Member States’ data protection authorities have criticised the very general formulation of the principles and the high reliance on self-certification and self-regulation. Similar concerns have been raised by industry, referring to distortions of competition due to a lack of enforcement.

The current Safe Harbour arrangement is based on the voluntary adherence of companies, on self-certification by these adhering companies and on enforcement of the self-certification commitments by public authorities. In this context any lack of transparency and any shortcomings in enforcement undermine the foundations on which the Safe Harbour scheme is constructed.

Any gap in transparency or in enforcement on the US side results in responsibility being shifted to European data protection authorities and to the companies which use the scheme. On 29 April 2010 German data protection authorities issued a decision requesting companies transferring data from Europe to the US to actively check that companies in the US importing data actually comply with Safe Harbour Privacy Principles and recommending that “at least the exporting company must determine whether the Safe Harbour certification by the importer is still valid”\(^{17}\).

On 24 July 2013, following the revelations on US surveillance programmes, German DPAs went a step further expressing concerns that “there is a substantial likelihood that the principles in the Commission’s decisions are being violated”\(^{18}\). There are cases of some DPAs (e.g., Bremen DPA) that have requested a company transferring personal data to US providers to inform the DPA on whether and how the concerned providers prevent access by the National Security Agency. The Irish DPA has reported that it received two complaints recently which reference the Safe Harbour programme following coverage about the US Intelligence Agencies programmes but declined to investigate them on the basis that the transfer of personal data to a third country met the requirements of Irish data protection law. Following a similar complaint, the Luxembourg DPA has found that Microsoft and Skype have complied with the Luxembourg Data Protection Act when transferring data to US\(^{19}\). However, the Irish High Court has since granted an application for judicial review under which it will review the inaction of the Irish Data Protection Commissioner in relation to the US surveillance programmes. One of the two complaints was filed by a student group Europe v Facebook (EvF) which also filed similar complaint against Yahoo in Germany, which is being processed by the relevant data protection authorities.

These divergent responses of data protection authorities to the surveillance revelations demonstrate the real risk of the fragmentation of the Safe Harbour scheme and raise questions as to the extent to which it is enforced.

---

\(^{16}\) Safe Harbour organizations that cover organization human resources data under their Safe Harbour certification (and thereby have agreed to cooperate and comply with the EU data protection authorities): 51% (1671 of 3246).


\(^{18}\) See a resolution of a German Conference of data protection commissions underlying that intelligence services constitute a massive threat to data traffic between Germany and countries outside Europe: [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIEBE_PH_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Speeches/2013/13-10-07_Speech_LIEBE_PH_EN.pdf)

\(^{19}\) See the press statement of Luxemboug DPA on 18 November 2013.
3. Transparency of Adhered Companies’ Privacy Policies

Under the FAQ 6 that is annexed to the Safe Harbour Decision (Annex II) companies interested in certifying under the Safe Harbour must provide to the Department of Commerce and make public their privacy policy. It must include a commitment to adhere to the Privacy Principles. The requirement to make publicly available the privacy policies of self-certified companies as well as their statement to adhere to the Privacy Principles is critical for the operation of the scheme.

Insufficient accessibility to privacy policies of such companies is to the detriment of individuals whose personal data is being collected and processed, and may constitute a violation of the principle of notice. In such cases, individuals whose data is being transferred from the EU may be unaware of their rights and the obligations to which a self-certified company is subjected.

Moreover, the commitment by companies to comply with the Privacy Principles triggers the Federal Trade Commission’s powers to enforce these principles against companies in cases of non-compliance as an unfair or deceptive practice. Lack of transparency by companies in the US renders Federal Trade Commission oversight more difficult and undermines the effectiveness of enforcement.

Over the years a substantial number of self-certified companies had not made their privacy policy public and/or had not made a public statement of adherence to the Privacy Principles. The 2004 Safe Harbour report pointed to the necessity for the Department of Commerce to adopt a more active stance in scrutinising compliance with this requirement.

Since 2004, the Department of Commerce has developed new information tools aimed at helping companies to comply with their transparency obligations. The relevant information on the scheme is accessible on the Department of Commerce’s website dedicated to the Safe Harbour that also allows companies to upload their privacy policies. The Department of Commerce has reported that companies have made use of this feature and posted their privacy policies on the Department of Commerce website when applying to join the Safe Harbour.

In addition, the Department of Commerce published in 2009-2013 a series of guidelines for companies wishing to join Safe Harbour, such as a “Guide to Self-Certification” and “Helpful Hints on Self-Certifying Compliance”.

The degree of compliance with the transparency obligations varies amongst companies. Whereas certain companies limit themselves to notifying to the Department of Commerce a description of their privacy policy as part of the self-certification process, the majority make these policies public on their websites, in addition to uploading them on the Department of Commerce website. However, these policies are not always presented in a consumer-friendly and easily readable form. Hyperlinks to privacy policies do not always function properly nor do they always refer to the correct webpages.

It follows from the Decision and its annexes that the requirement that companies should publicly disclose their privacy policies goes beyond mere notification of self-certification to the Department of Commerce. The requirements for certification as set out in the FAQs include a description of the privacy policy and transparent information on where it is available for viewing by the public. Privacy policy statements must be clear and easily accessible by

---


21 [https://SafeHarbour.export.gov/list.aspx](https://SafeHarbour.export.gov/list.aspx)

22 The Guide is available on the programme’s website at: [http://export.gov/SafeHarbour/HelpfulHints.html](http://export.gov/SafeHarbour/HelpfulHints.html)

23 On 12 November 2013 the Department of Commerce has confirmed that “Today, companies that have public websites and cover consumer/client/visitor data must include a Safe Harbor-compliant privacy policy on their respective websites” (document: “U.S.-EU Cooperation to Implement the Safe Harbor Framework” of 12 Nov. 2013).
the public. They must include a hyperlink to the Department of Commerce Safe Harbour website which lists all the ‘current’ members of the scheme and a link to the alternative dispute resolution provider. However, a number of companies under the scheme in the period 2000-2013 failed to comply with these requirements. During working contacts with the Commission in February 2013 the Department of Commerce has acknowledged that up to 10% of certified companies may actually not have posted a privacy policy containing the Safe Harbour affirmative statement on their respective public websites.

Recent statistics demonstrate also a persisting problem of false claims of Safe Harbour adherence. About 10% of companies claiming membership in the Safe Harbour are not listed by the Department of Commerce as current members of the scheme\textsuperscript{24}. Such false claims originate from both: companies which have never been participants of the Safe Harbour and companies which have once joined the scheme but then failed to resubmit their self-certification to the Department of Commerce at the yearly intervals. In this case they continue to be listed on the Safe Harbour website, but with certification status "not current", meaning that the company has been a member of the scheme and thus has an obligation to continue to provide protection to data already processed. The Federal Trade Commission is competent to intervene in cases of deceptive practices and non-compliance of the Safe Harbour principles (see Section 5.1). Uncertainty over the "false claims" impacts the credibility of the scheme.

The European Commission alerted the Department of Commerce through regular contacts in 2012 and 2013 that, in order to comply with the transparency obligations, it is not sufficient for companies to only provide the Department of Commerce with a description of their privacy policy. Privacy policy statements must be made publicly available. The Department of Commerce was also asked to intensify its periodic controls of companies’ websites subsequent to the verification procedure carried out in the context of the first self-certification process or its annual renewal and to take action against those companies which do not comply with the transparency requirements.

As a first answer to EU concerns, the Department of Commerce has since March 2013 made it mandatory for a Safe Harbour company with a public website to make its privacy policy for customer/user data readily available on its public website. At the same time, the Department of Commerce began notifying all companies whose privacy policy did not already include a link to Department of Commerce Safe Harbour website that one should be added, making the official Safe Harbour List and website directly accessible to consumers visiting a company’s website. This will allow European data subjects to verify immediately, without additional searches in the web, a company’s commitments submitted to the Department of Commerce. Additionally, the Department of Commerce started notifying companies that contact information for their independent dispute resolution provider should be included in their posted privacy policy\textsuperscript{25}.

This process needs to be speeded up to ensure that all certified companies fully meet Safe Harbour requirements not later than by March 2014 (i.e. by companies’ yearly recertification deadline, counting from the introduction of new requirements in March 2013).

\textsuperscript{24} In September 2013 an Australian consultancy Galexia compared Safe Harbour membership "false claims" in 2008 and 2013. Its main finding is that, in parallel to the increase of membership in the Safe Harbour between 2008 and 2013 (from 1,109 to 3,246), the number of false claims has increased from 206 to 427. http://www.galexia.com/public/about/news/about_news-id225.html

\textsuperscript{25} Between March and September 2013 the Department of Commerce has:

• Notified the 101 companies who had already uploaded their Safe Harbour compliant privacy policy to Safe Harbour website that they must also post their privacy policy to their company websites;
• Notified the 154 companies that had not already done so, that they should include a link to Safe Harbour website in their privacy policy;
• Notified more than 600 companies that they should include contact information for their independent dispute resolution provider in their privacy policy.
Nevertheless, concerns remain as to whether all self-certified companies fully comply with the transparency requirements. Compliance with the obligations undertaken at the point of the initial self-certification and the annual renewal should be monitored and investigated more stringently by the Department of Commerce.

4. **Integration of the Safe Harbour Privacy Principles in Companies’ Privacy Policies**

Self-certified companies must comply with the Privacy Principles set out in Annex I to the Decision in order to obtain and retain the benefit of the Safe Harbour.

In the 2004 report, the Commission found that a significant number of **companies had not correctly incorporated the Safe Harbour Privacy Principles** in their data processing policies. For example, individuals were not always given clear and transparent information about the purposes for which their data were processed or were not given the possibility to opt out if their data were to be disclosed to a third party or to be used for a purpose that was incompatible with the purposes for which it was originally collected. The 2004 Commission's report considered that the Department of Commerce “should be more proactive with regard to access to the Safe Harbour and to awareness of the Principles”.

There has been limited progress in that respect. Since 1 January 2009, any company seeking to renew its certification status for Safe Harbour – which must be renewed annually – has had its privacy policy evaluated by the Department of Commerce prior to the renewal. The evaluation is however limited in scope. There is no full evaluation of the actual practice in the self-certified companies which would significantly increase the credibility of the self-certification process.

Further to the Commission's requests for a more rigorous and systematic oversight of the self-certified companies by the Department of Commerce, **more attention is currently applied to new submissions**. The number of new submissions which have not been accepted, but are resent to companies for improvements in privacy policies has significantly increased between 2010 and 2013: doubled for re-certifying companies and tripled for the Safe Harbour newcomers. The Department of Commerce has assured the Commission that any certification or recertification can be finalised only if the company’s privacy policy fulfils all requirements, notably that it includes an affirmative commitment to adhere to the relevant set of Safe Harbour Privacy Principles and that the privacy policy is publicly available. A company is required to identify in its Safe Harbour List record the location of the relevant policy. It is also required to clearly identify on its website an Alternative Dispute Resolution provider and include a link to the Safe Harbour self-certification on the website of the Department of Commerce. However, it has been estimated that over 30% of Safe Harbour members do not provide dispute resolution information in the privacy policies on their websites.

A majority of the companies that the Department of Commerce has removed from the Safe Harbour List were removed at the express request of the relevant companies (e.g., companies that had merged or were acquired, had changed their lines of business or had gone out of business). A smaller number of records of lapsed companies have been removed when the

---


According to statistics provided in September 2013 by the Department in Commerce, the DoC notified in 2010 18% (93) of the 512 first-time certifiers and 16% (231) of the 1,417 recertifiers to make improvements to their privacy policies and/or Safe Harbour applications. However, as a follow up to Commission requests for severe, diligent and systematic scrutiny of all submissions, through mid-Sep. 2013, DoC notified 56% (340) of the 602 first-time certifiers and 27% (493) of the 1,809 recertifiers asking them to make improvements to their privacy policies.

Chris Connolly (Galexia) appearance before the European Parliament LIBE Committee inquiry on 7 Oct. 2013.
websites that were listed in the records appeared to be inoperative and the companies’ certification status had been “Not current” for several years. Importantly, none of these removals seems to have taken place because the Department of Commerce verification led to the identification of compliance problems.

The Safe Harbour List record serves as a public notice and as a record of a company’s Safe Harbour commitments. The commitment to adhere to the Safe Harbour Principles is not time-limited with respect to data received during the period in which the company enjoys the benefit of the Safe Harbour, and the company must continue to apply the Principles to such data as long as it stores, uses or discloses them, even if it leaves the Safe Harbour for any reason.

The number of Safe Harbour applicants that did not pass administrative review by the Department of Commerce and therefore were never added to the Safe Harbour List is the following: In 2010, only 6% (33) of the 513 first-time certifiers were never included in the Safe Harbour List because they did not comply with Department of Commerce standards for self-certification. In 2013, 12% (75) of the 605 first-time certifiers were never included in the Safe Harbour List because they have not complied with Department of Commerce standards for self-certification.

As a minimum requirement to increase the transparency of the oversight, the Department of Commerce should list on its website all companies that have been removed from the Safe Harbour and indicate reasons for which the certification has not been renewed. The label “Not current” on the Department of Commerce list of Safe Harbour member companies should be regarded not just as information but should be accompanied by a clear warning – both verbal and graphical - that a company is currently not fulfilling Safe Harbour requirements.

Moreover, some companies still fall short of fully incorporating all Safe Harbour Principles. Apart from the issue of transparency addressed in Section 3 above, privacy policies of self-certified companies are often unclear as regards the purposes for which data is collected, and the right to choose whether or not data can be disclosed to third parties; thereby raising issues of compliance with the Privacy Principles of “Notice” and “Choice”. Notice and choice are crucial to ensure control from data subjects over what happens to their personal information.

The critical first step in the compliance process, the incorporation of the Safe Harbour Privacy Principles in companies' privacy policies, is not sufficiently ensured. The Department of Commerce should address it as a matter of priority by developing a methodology of compliance in the operational practice of companies and their interaction with clients. There must be an active follow up by the Department of Commerce on effective incorporation of the Safe Harbour principles in companies' privacy policies, rather than leaving enforcement action only to be triggered by complaints of individuals.

5. **ENFORCEMENT BY PUBLIC AUTHORITIES**

A number of mechanisms are available to ensure effective enforcement of the Safe Harbour scheme and to offer recourse for individuals in cases where the protection of their personal information is affected by non-compliance with the Privacy Principles.

According to the “Enforcement” Principle, privacy policies of self-certified organizations must include effective compliance mechanisms. Pursuant to the “Enforcement” Privacy Principle as further clarified by FAQ 11, FAQ 5 and FAQ 6, this requirement can be met by

---

29 As of December 2011, the US Department of Commerce had removed 323 companies from the Safe Harbour List: 94 companies were removed because they were no longer in business; 88 companies due to acquisition or merger, 95 at the requests of the parent company; 41 companies because repeated failure to ask for recertification and 5 companies for miscellaneous reasons.
adhering to independent recourse mechanisms that have publicly stated their competence to hear individual complaints for failure to abide by the Principles. Alternatively, this can be achieved through the organization’s commitment to cooperate with the EU Data Protection Panel\textsuperscript{30}. Moreover self-certified companies are subject to the jurisdiction of the Federal Trade Commission under Section 5 of the Federal Trade Commission Act which prohibits unfair or deceptive acts or practices in or affecting commerce\textsuperscript{31}.

The 2004 Report expressed concerns as regards the enforcement of the Safe Harbour scheme, namely that the Federal Trade Commission should be more proactive in launching investigations and raising awareness of individuals about their rights. Another area of concern was the lack of clarity in relation to the Federal Trade Commission's competence to enforce the Principles regarding human resources data.

The recourse body responsible for human resources data – the EU Data Protection Panel – has received one complaint concerning human resources data\textsuperscript{32}. However, the absence of complaints does not allow conclusions to be drawn as to the full functioning of the scheme. Ex-officio checks of companies’ compliance should be introduced to verify the actual implementation of data protection commitments. EU Data Protection Authorities should also undertake actions in order to raise awareness of the existence of the Panel.

Problems have been highlighted in relation to the way in which alternative recourse mechanisms function as enforcement bodies. A number of these bodies lack appropriate means to remedy cases of failure to comply with the Principles. This shortcoming needs to be addressed.

5.1. Federal Trade Commission

The Federal Trade Commission can take enforcement measures in case of violations of the Safe Harbour commitments that companies make. When Safe Harbour was established, the Federal Trade Commission committed to review on a priority basis all referrals from EU Member State authorities\textsuperscript{33}. Since no complaints were received for the first ten years of the arrangement, the Federal Trade Commission decided to seek to identify any Safe Harbour violations in every privacy and data security investigation it conducts. Since 2009, the Federal Trade Commission has brought 10 enforcement actions against companies based on Safe Harbour violations. These actions notably resulted in settlement orders – subject to substantial penalties – prohibiting privacy misrepresentations, including of compliance with the Safe Harbour, and imposing on companies’ comprehensive privacy programmes and audits for 20 years. The companies must accept independent assessments of their privacy programmes on the request of the Federal Trade Commission. These assessments are reported regularly to the Federal Trade Commission. The Federal Trade Commission's orders also prohibit these companies from misrepresenting their privacy practices and their participation in Safe Harbour or similar privacy schemes. This was the case for example in the Federal Trade

---

\textsuperscript{30} The EU Data Protection Panel is a body competent for investigating and resolving complaints lodged by individuals for alleged infringement of the Safe Harbour Principles by an US company member of the Safe Harbour. Companies that certify to the Safe Harbour Principles must choose to comply with independent recourse mechanism or to cooperate with the EU Data Protection Panel in order to remedy problems arising out of failure to comply with Safe Harbour Principles. Cooperation with the EU Data Protection Panel is nonetheless mandatory when the US company processes human resources personal data transferred from the EU in the context of an employment relationship. If the company commits itself to cooperate with the EU panel, it must also commit itself to comply with any advice given by the EU panel where it takes the view that the company needs to take specific action to comply with the Safe Harbour Principles, including remedial or compensatory measures.

\textsuperscript{31} The Department of Transportation exercises similar jurisdictions over air carriers under Title 49 United States Code Section 41712.

\textsuperscript{32} The complaint originated from a Swiss citizen and therefore has been referred by the EU Data Protection Panel to the Swiss data protection authority (US has a separate Safe Harbour scheme for Switzerland).

Commission investigations against Google, Facebook and Myspace. In 2012 Google agreed to pay a $22.5 million fine to settle allegations that it violated a consent order. In all privacy investigations the Federal Trade Commission ex officio examines whether there is Safe Harbour violation.

The Federal Trade Commission has reiterated recently its declarations and commitment to reviewing, on a priority basis, any referrals received from privacy self-regulatory companies and EU Member States that allege a company’s non-compliance with Safe Harbour Principles. The Federal Trade Commission has received only a few referrals from European data protection authorities over the past three years.

Transatlantic cooperation between data protection authorities started to develop in recent months. For example the Federal Trade Commission signed on 26 June 2013 with the Office of the Data Protection Commissioner of Ireland a Memorandum of Understanding on mutual assistance in the enforcement of laws protecting personal information in the private sector. The memorandum establishes a framework for increased, more streamlined, and more effective privacy enforcement cooperation.

In August 2013, the Federal Trade Commission announced a further reinforcement of the checks on companies with control over large databases of personal information. It has also created a portal where consumers can file a privacy complaint regarding a US company.

The Federal Trade Commission should also increase efforts to investigate false claims of Safe Harbour adherence. A company claiming on its website that it complies with the Safe Harbour requirements, but is not listed by the Department of Commerce as a ‘current’ member of the scheme, is misleading consumers and abusing their trust. False claims weaken the credibility of the system as a whole and therefore should be immediately removed from the companies’ websites. The companies should be bound by an enforceable requirement not to mislead consumers. The Federal Trade Commission should continue seeking to identify Safe Harbour false claims as in the one in the Karnani case, where the Federal Trade Commission shut down a California website for claiming a false Safe Harbour registration, and engaging in fraudulent e-commerce practices targeted at European consumers.

On 29 October 2013 the Federal Trade Commission announced that it had opened “numerous investigations into Safe Harbor compliance in recent months” and that more enforcement actions on this front can be expected “in the coming months”. The Federal Trade Commission confirmed also that it is "committed to looking for ways to improve its efficacy" and would “continue to welcome any substantive leads, such as the complaint received in the past month from a European-based consumer advocate alleging a large number of Safe Harbor-related violations”. The agency committed also to “systematically monitor compliance with Safe Harbor orders, as we do with all our orders.”

---


35 This commitment has been reiterated at a meeting of Federal Trade Commission Commissioner Julie Brill with EU Data protection Authorities (Article 29 Working Party) in Brussels on 17 April 2013.

36 http://www.dataprotection.ie/viewdoc.asp?Docid=1317&Catid=66&StartDate=1+January+2013&m=n

37 Consumers can file their complaints via the Federal Trade Commission Complaint Assistant (https://www.ftc.complaintassistant.gov/) and international consumers may file complaints via econsumer.gov (http://www.econsumer.gov).


40 Letter of the Federal Trade Commission Chairwoman Edith Ramirez to Vice-President Viviane Reding.
On 12 November 2013, the Federal Trade Commission informed the European Commission that “if a company’s privacy policy promises Safe Harbor protections, that company’s failure to make or maintain a registration, is not, by itself, likely to excuse that company from FTC enforcement of those Safe Harbor commitments”\(^{41}\).

In November 2013, the Department of Commerce informed the European Commission that “to help ensure that companies do not make ‘false claims’ of participation in Safe Harbor, the Department of Commerce will begin a process of contacting Safe Harbor participants one month prior to their recertification date to describe the steps they must follow should they chose not to recertify”. The Department of Commerce “will warn companies in this category to remove all references to Safe Harbor participation, including use of Commerce’s Safe Harbor certification mark, from the companies’ privacy policies and websites, and notify them clearly that failure to do so could subject the companies to FTC enforcement actions”\(^{42}\).

To combat false claims of Safe Harbour adherence, privacy policies of self-certified companies’ websites should always include a link to the Department of Commerce Safe Harbour website where all the ‘current’ members of the scheme are listed. This will allow European data subjects to verify immediately, without additional searches whether a company is currently a member of the Safe Harbour. The Department of Commerce has started in March 2013 to request this from companies, but the process should be intensified.

The continuous monitoring and consequent enforcement by the Federal Trade Commission of actual compliance with the Safe Harbour Principles – in addition to the measures taken by the Department of Commerce as highlighted above – remains a key priority for ensuring proper and effective functioning of the scheme. It is necessary in particular to increase \textit{ex-officio checks and investigations of companies’ compliance} to the Safe Harbour principles. Complaints to the Federal Trade Commission relating violations should also be further facilitated.

5.2. EU Data Protection Panel

The EU Data Protection Panel is a body created under the Safe Harbour Decision. It is competent to investigate complaints lodged by individuals referring to personal data collected in the context of the employment relationship as well as cases relating to certified companies which have chosen this option for dispute resolution under the Safe Harbour (53% of all companies). It is composed of representatives of various EU data protection authorities.

To date, the Panel received four complaints (two in 2010 and two in 2013). It referred two complaints in 2010 to national data protection authorities (UK and Switzerland). The third and the fourth complaints are currently under examination. The low level of complaints can be explained by the fact that the powers of Panel are, as mentioned above, primarily limited to certain type of data.

The Panel's limited caseload could be also partly explained by the lack of awareness about the existence of the Panel. The Commission has, since 2004, made the information about the Panel more visible on its website\(^{43}\).

---

\(^{41}\) Letter of the Federal Trade Commission Chairwoman Edith Ramirez to Vice-President Viviane Reding.


\(^{43}\) Pursuant to the 2004 report, an Information Notice in the form of Q&A of the EU Data Protection Panel has been published on the Commission’s website (DG Justice) with the purpose of raising awareness of individuals and help them to file a complaint when they believe that their personal data has been processed in violation of the Safe Harbour: [http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/adequacy/information_Safe_harbour_en.pdf)

The standard complaint form is available at [http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/adequacy/complaint_form_en.pdf)
To make a better use of the Panel, companies in the US which have chosen to cooperate with it and comply with its decisions, for some or all categories of personal data covered in their respective self-certifications, should clearly and prominently indicate it in their privacy policies commitments to allow the Department of Commerce to scrutinise this aspect. A dedicated page should be created on each EU data protection authority's website regarding Safe Harbour to raise Safe Harbour awareness with European companies and data subjects.

5.3. Improvement of enforcement

The weaknesses in transparency and weaknesses in enforcement that have been identified above, lead to concerns among European companies as regards the negative impact of the Safe Harbour scheme on European companies' competitiveness. Where a European company competes with a US company operating under Safe Harbour, but in practice not applying its principles, the European company is at a competitive disadvantage in relation to that US company.

Furthermore, the Federal Trade Commission's jurisdiction extends to unfair or deceptive acts or practices "in or affecting commerce". Section 5 of the Federal Trade Commission Act established exceptions to the Federal Trade Commission's authority over unfair or deceptive acts or practices with respect inter alia to telecommunications. Being outside Federal Trade Commission enforcement, telecom companies are not allowed to adhere to the Safe Harbour. However, with the growing convergence of technologies and services, many of their direct competitors in the US ICT sector are members of Safe Harbour. The exclusion of telecom companies from the data exchanges under the Safe Harbour scheme is a matter of concern to some European telecom operators. According to the European Telecommunications Network Operators’ Association (ETNO) “this is in clear conflict to the most important plea of telecommunication operators regarding the need for a level playing field” 44.

6. Strengthening the Safe Harbour Privacy Principles

6.1. Alternative Dispute Resolutions

The enforcement principle requires that there must be “readily available and affordable recourse mechanisms by which each individual’s complaints and disputes are investigated”. To that end the Safe Harbour scheme establishes a system of Alternative Dispute Resolution (ADR) by an independent third party 45 to provide individuals with rapid solutions. The three top recourse mechanisms bodies are the EU Data Protection Panel, BBB (Better Business Bureaus) and TRUSTe.

44 “ETNO considerations” received by Commission services on 4 October 2013 discuss also 1) definition of personal data in Safe Harbour, 2) lack of monitoring of the Safe Harbour, 3) and the fact that “US companies can transfer data with much less restrictions than their European counterparts” which “constitutes a clear discrimination of European companies and is affecting the competitiveness of European companies”. Under the Safe Harbour rules, to disclose information to a third party, organizations must apply the Notice and Choice Principles. Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.

45 The EU Directive 2013/11/EU on consumer ADR underlines the importance of independent, impartial, transparent, effective, fast and fair alternative dispute resolution procedures.
The use of ADR has increased since 2004 and the Department of Commerce has strengthened the monitoring of American ADR providers to make sure that the information they offer about the complaint procedure is clear, accessible and understandable. However, the effectiveness of this system is yet to be proven due to the limited number of cases dealt with so far.\textsuperscript{46}

Though the Department of Commerce has been successful is reducing the fees charged by the ADRs, two out of seven major ADR providers continue to charge fees from individuals who file a complaint\textsuperscript{47}. This represents the ADR providers used by about 20\% of Safe Harbour companies. These companies have selected an ADR provider that charges a fee to consumers for filing a complaint. Such practices do not comply with the Enforcement Principle of Safe Harbour which gives individuals the right of access to a "readily available and affordable independent recourse mechanisms". In the European Union, access to an independent dispute resolution service provided by the EU Data Protection Panel is free for all data subjects.

On 12 November 2013 the Department of Commerce confirmed that it "will continue to advocate on behalf of EU citizens' privacy and work with ADR providers to determine whether their fees can be lowered further".

In relation to sanctions, not all ADR providers possess the necessary tools to remedy situations of failure to abide by the Privacy Principles. Moreover, the publication of findings

\textsuperscript{46} For example, one major service provider ("TRUSTe") reported that it received 881 requests in 2010, but that only three of them were considered admissible, and grounded, and led to the company concerned being required to change its privacy policy and website. In 2011, the number of complaints was 879, and in one case the company was required to change its privacy policy. According to the DoC, vast majority of the complaints to ADR are requests from consumers, for example users who have forgotten their password and were unable to obtain it from the internet service. Following Commission requests, the Department of Commerce developed new statistics reporting criteria to be used by all ADR. They distinguish between mere requests and complaints and they provide with further clarification of types of complaints received. These new criteria need however to be further discussed to make sure that new statistics in 2014 concern all ADR providers, are comparable and provide critical information to assess the effectiveness of the recourse mechanism.

\textsuperscript{47} International Centre for Dispute Resolution / American Arbitration Association (ICDR/AAA), charges $ 200 and JAMS $ 250 “filing fee”. The Department of Commerce informed the Commission that it had worked with the AAA, the most costly dispute resolution provider for individuals, to develop a Safe Harbour-specific program which reduced the cost to consumers from several thousands of dollars to a flat rate of $ 200.
of non-compliance does not seem to be foreseen amongst the range of sanctions and measures of all ADR service providers.

ADR providers are also required to refer cases to the Federal Trade Commission where a company fails to comply with the outcome of the ADR process, or rejects the ADR provider's decision, so that the Federal Trade Commission can review and investigate and, if appropriate, take enforcement measures. However, to date, there have been no cases of referral from ADR providers to the Federal Trade Commission for non-compliance.\(^\text{48}\)

Alternative dispute resolution service providers maintain on their Websites lists of companies (Dispute Resolution Participants) which use their services. This allows consumers to easily verify if – in case of dispute with a company – an individual can submit a complaint to an identified dispute resolution provider. Thus, for example the BBB dispute resolution provider lists all companies which are under the BBB dispute resolution system. However, there are numerous companies claiming to be under a specific dispute resolution system but not listed by the ADR service providers as participants of their dispute resolution scheme\(^\text{49}\).

ADR mechanisms should be easily accessible, independent and affordable for individuals. A data subject should be able to file a complaint without any excessive constraints. All ADR bodies should publish on their websites statistics about the complaints handled as well as specific information about their outcome. Finally, the ADR bodies should be further monitored to make sure that information they provide about the procedure and how to lodge a complaint is clear and understandable, so that the dispute resolution becomes an effective, trusted mechanism providing results. It should also be reiterated that publication of findings of non-compliance should be included within the range of mandatory sanctions of ADRs.

6.2. Onward transfer

With the exponential growth of data flows there is a need to ensure the continued protection of personal data at all stages of data processing, notably when data is transferred by a company adhering to the Safe Harbour to a third party processor. Therefore, the need for the better enforcement of the Safe Harbour concerns not only Safe Harbour members but also subcontractors.

The Safe Harbour scheme allows onward transfers to third parties acting as “agents” if the company – member of the Safe Harbour scheme – “ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the Privacy Principles”.\(^\text{50}\) For example, a cloud service provider is required by the Department of Commerce to enter into a contract even if it is “Safe Harbour-compliant” and it receives personal data for processing.\(^\text{51}\) However, this provision is not clear in Annex II to the Safe Harbour Decision.

As the recourse to subcontractors has increased considerably over the past years, in particular in the context of cloud-computing, when entering such a contract, a Safe Harbour company

\(^{48}\) See FAQ 11.

\(^{49}\) Examples: Amazon has informed the DoC that it uses the BBB as its dispute resolution provider. However the BBB does not list Amazon among its dispute resolution participants. Vice versa, Arsalon Technologies (www.arsalon.net), a cloud hosting service provider, appears on the BBB Safe Harbour dispute resolution list but the company is not a current member of the Safe Harbour (situation as of 1 October 2013). BBB, TRUSTe and other ADR service providers should remove or correct the certification claims. They should be bound by an enforceable requirement to only certify companies who are members of the Safe Harbour.

\(^{50}\) See Commission Decision 2000/520/EC page 7 (onward transfer).

should notify the Department of Commerce and be obliged to make public the privacy safeguards.\(^{52}\)

The three above mentioned issues: the alternative dispute resolution mechanism, reinforced oversight and onward transfers of data should be further clarified.

7. **ACCESS TO DATA TRANSFERRED IN THE FRAMEWORK OF THE SAFE HARBOR SCHEME**

In the course of 2013, information on the scale and scope of US surveillance programmes has raised concerns over the continuity of protection of personal data lawfully transferred to the US under the Safe Harbour scheme. For instance, all companies involved in the PRISM programme, and which grant access to US authorities to data stored and processed in the US, appear to be Safe Harbour certified. This has made the Safe Harbour scheme one of the conduits through which access is given to US intelligence authorities to collecting personal data initially processed in the EU.

The Safe Harbour Decision provides, in Annex 1, that adherence to the Privacy Principles may be limited, if justified by national security, public interest, or law enforcement requirements or by statute, government regulation or case-law. In order for limitations and restrictions on the enjoyment of fundamental rights to be valid, they must be narrowly construed; they must be set forth in a publicly accessible law and they must be necessary and proportionate in a democratic society. In particular, the Safe Harbour Decision specifies that such limitations are allowed only “to the extent necessary” to meet national security, public interest, or law enforcement requirements.\(^{53}\) While the exceptional processing of data for the purposes of national security, public interest or law enforcement is provided under the Safe Harbour scheme, the large scale access by intelligence agencies to data transferred to the US in the context of commercial transactions was not foreseeable at the time of adopting the Safe Harbour.

Moreover, for reasons of transparency and legal certainty, the European Commission should be notified by the Department of Commerce of any statute or government regulations that would affect adherence to the Safe Harbour Privacy Principles.\(^{54}\) The use of exceptions should be carefully monitored and the exceptions must not be used in a way that undermines the protection afforded by the Principles.\(^{55}\) In particular, large scale access by US authorities to data processed by Safe Harbour self-certified companies risks undermining the confidentiality of electronic communications.

\(^{52}\) These remarks concern cloud providers which are not in the Safe Harbour. According to Galexia consultancy firm, “the level of Safe Harbour membership (and compliance) amongst cloud service providers is quite high. Cloud service providers typically have multiple layers of privacy protection, often combining direct contracts with clients and over-arching privacy policies. With one or two important exceptions, cloud service providers in the Safe Harbour are compliant with the key provisions relating to dispute resolution and enforcement. There are no major cloud service providers in the list of false membership claims at this time.” (appearance of Chris Connolly from Galexia before the LIBE Committee inquiry on “Electronic mass surveillance of EU citizens”).

\(^{53}\) See Annex 1 of the Safe Harbour Decision: “Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization; or (c) if the effect of the Directive of Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection where possible.”


7.1. Proportionality and necessity

As results from the findings of the ad hoc EU-US Working Group on data protection, a number of legal bases under US law allow large-scale collection and processing of personal data that is stored or otherwise processed companies based in the US. This may include data previously transferred from the EU to the US under the Safe Harbour scheme, and it raises the question of continued compliance with the Safe Harbour principles. The large scale nature of these programmes may result in data transferred under Safe Harbour being accessed and further processed by US authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in the Safe Harbour Decision.

7.2. Limitations and redress possibilities

As results from the findings of the ad hoc EU-US Working Group on data protection, safeguards that are provided under US law are mostly available to US citizens or legal residents. Moreover, there are no opportunities for either EU or US data subjects to obtain access, rectification or erasure of data, or administrative or judicial redress with regard to collection and further processing of their personal data taking place under the US surveillance programmes.

7.3. Transparency

Companies do not systematically indicate in their privacy policies when they apply exceptions to the Principles. The individuals and companies are thus not aware of what is being done with their data. This is particularly relevant in relation with the operation of the US surveillance programmes in question. As a result, Europeans whose data are transferred to a company in the US under Safe Harbour may not be made aware by those companies that their data may be subject to access\(^56\). This raises the question of compliance with the Safe Harbour principles on transparency. Transparency should be ensured to the greatest extent possible without jeopardising national security. In addition to existing requirements on companies to indicate in their privacy policies where the Principles may be limited by statute, government regulation or case law, companies should also 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.

8. CONCLUSIONS AND RECOMMENDATIONS

Since its adoption in 2000, Safe Harbour has become a vehicle for EU-US flows of personal data. The importance of efficient protection in case of transfers of personal data has increased due to the exponential increase in data flows central to the digital economy and the very significant developments in data collection, processing and use. Web companies such as Google, Facebook, Microsoft, Apple, Yahoo have hundreds of millions of clients in Europe and transfer personal data for processing to the US on a scale inconceivable in the year 2000 when the Safe Harbour was created.

\(^{56}\) Relatively transparent information in this respect is provided by some European companies in Safe Harbour. For example Nokia, which has operations in the US and is a Safe Harbour member provides a following notice in its privacy policy: “We may be obligated by mandatory law to disclose your personal data to certain authorities or other third parties, for example, to law enforcement agencies in the countries where we or third parties acting on our behalf operate.”
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.

On the basis of the above, the Commission has identified the following recommendations:

**Transparency**

1. **Self-certified companies should publicly disclose their privacy policies.** It is not sufficient for companies to provide the Department of Commerce with a description of their privacy policy. Privacy policies should be made publicly available on the companies' websites, in clear and conspicuous language.

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.** This will allow European data subjects to verify immediately, without additional searches whether a company is currently a member of the Safe Harbour. This would help increase the credibility of the scheme by reducing the possibilities for false claims of adherence to the Safe Harbour. The Department of Commerce has started in March 2013 to request this from companies, but the process should be intensified.

3. **Self-certified companies should publish privacy conditions of any contracts they conclude with subcontractors, e.g. cloud computing services.** Safe Harbour allows onward transfers from Safe Harbour self-certified companies to third parties acting as “agents”, for example to cloud service providers. According to our understanding, in such cases the Department of Commerce requires from self-certified companies to enter into a contract. However, when entering such a contract, a Safe Harbour company should also notify the Department of Commerce and be obliged to make public the privacy safeguards.

4. **Clearly flag on the website of the Department of Commerce all companies which are not current members of the scheme.** The label “Not current” on the Department of Commerce list of Safe Harbour members should be accompanied by a clear warning that a company is currently not fulfilling Safe Harbour requirements. However, in the case of "Not current" the company is obliged to continue to apply the Safe Harbour requirements for the data that has been received under Safe Harbour.

**Redress**

5. **The privacy policies on companies’ websites should include a link to the alternative dispute resolution (ADR) provider and/or EU panel.** This will allow European data subjects to contact immediately the ADR or EU panel in case of problems. Department of Commerce has started in March 2013 to request this from companies, but the process should be intensified.
6. **ADR should be readily available and affordable.** Some ADR bodies in the Safe Harbour scheme continue to charge fees from individuals – which can be quite costly for an individual user – for the handling of the complaint ($200-250). By contrast, in Europe access to the Data Protection Panel foreseen for solving complaints under the Safe Harbour, is free.

7. **Department of Commerce should monitor more systematically ADR providers regarding the transparency and accessibility of information they provide concerning the procedure they use and the follow-up they give to complaints.** This makes the dispute resolution an effective, trusted mechanism providing results. It should also be reiterated that publication of findings of non-compliance should be included within the range of mandatory sanctions of ADRs.

**Enforcement**

8. **Following the certification or recertification of companies under the 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.** A company claiming on its website that it complies with the Safe Harbour requirements, but is not listed by the Department of Commerce as a ‘current’ member of the scheme, is misleading consumers and abusing their trust. False claims weaken the credibility of the system as a whole and therefore should be immediately removed from the companies’ websites.

**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.**