Ref. Ares(2014)1139376 - 10/04/2014

ARTICLE 29 Data Protection Working Party

Brussels, 10 April 2014

Viviane Reding
Vice President
Commissioner for Justice, Fundamental
Rights and Citizenship
European Commission
B - 1049 BRUSSELS Belgium

Dear Vice President Reding,

The Article 29 Working Party ("WP29") welcomes the actions set out by the European Commission in order to restore trust in data flows between the EU and the US, which were released on 27 November 2013.

Taking into account the political importance of the Safe Harbor, influenced by the constant evolution of technologies, interrogations on the Safe Harbor safeguards that are regularly submitted to national data protection authorities by EU organizations, the current discussions on the data protection reform and the revelations on mass State surveillance by US security authorities, improvements to Safe Harbor have become highly necessary.

The WP 29 has taken note of the opinion the European Parliament expressed in its resolution of 12 March 2014 on the US NSA surveillance program, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs (2013/2188(INI)), paragraph 38 and supports the idea that under the current circumstances, the possibility for Safe Harbor to provide adequate protection for EU citizens is questionable. Therefore the Working Party recognizes that if the revision process currently undertaken by European Commission does not lead to a positive outcome, then the Safe Harbor agreement should be suspended. In any case, the Working Party recalls that data protection authorities may suspend data flows according to their national competence and EU law.

The WP29 agrees that restoring trust in EU-US transfers cannot take place without strengthening the safeguards provided by the Safe Harbor. In this regard, it looked into the recommendations issued in the Communication on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU (COM(2013) 847 final). The WP29 welcomes the initiative of the European Commission and supports all of the recommendations issued in its Communication and, in particular, recommendations 12 and 13.

In the context of the current discussions between the EU Commission and the US authorities to adapt the Safe Harbor framework, the WP29 would like to take the opportunity to point out some additional elements that should be improved in the Safe Harbor Decision. The WP29 proposes that these additional recommendations (see Appendix) are used by the European Commission in its ongoing negotiations with the US, with a view to efficiently protecting EU data subjects whose personal data are transferred under the Safe Harbor framework.

The knowledge gathered on the practical implications of the current Safe Harbor framework also makes the WP 29 believe that its consultation on any proposal to modify the Safe Harbor framework will be valuable to the European Commission. The improvements to the Safe Harbor that will be made by the US in the upcoming months need to be sufficient to restore trust and the WP29 remains available for any further input on this matter and appreciates the Commission`s intention to keep us informed of developments during the negotiations.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chair

cc:
Cecilia Malmström, Commissioner for Home Affairs
Martin Schulz, President of the European Parliament
Juan Fernando López Aguilar, Chairman of the LIBE Committee of the European Parliament

Appendix: WP29 additional recommendations to strengthen personal data protection under the Safe Harbor Decision

The WP29 repeats its complete support to all of the recommendations already issued by the European Commission in its Communication. The WP29 lists here additional recommendations that need to be taken into consideration for the necessary guarantees provided by the Safe Harbor to sufficiently protect personal data transferred from the EU.

As a general comment, the WP29 notes that some requirements set out by the Safe Harbor Decision are only contained in the Frequently Asked Questions (hereinafter "FAQs") but do not appear at all in the Safe Harbor Privacy Principles (hereinafter "the Principles")[1]. Such dispersal of the requirements makes it more difficult for organizations to identify and comply with them, and hence, makes the protection adduced by the Safe Harbor decision less efficient and protective as regards data subjects.

As a consequence, the requirements should all be contained in the Principles, while the FAQs should only be aimed at providing further explanations on the Principles.

Furthermore, in order to prevent confusion over the obligations enshrined in the Safe Harbor Agreement, a clearer guidance should be provided on the mechanisms as well as the meaning of the Safe Harbor data protection principles. Such guidance can be the result of an improved and comprehensive structure of the Safe Harbor principles, which can be subdivided in numbered provisions to include also the relevant FAQs for each principle.

Applicable law

The Working Party suggests to clarify the fact that under the Directive (Article 4.1) Member States laws apply not only to the processing operations carried out by data controllers established on their territory, but also where data controllers (although not being established in the EU), make use of equipment situated on such territory in particular for the collection of personal data.

As a consequence, a Safe Harbor organization, acting as a controller, which is not established in the EU but which is collecting personal data with equipment situated in the EU is under the duty to apply EU Member states law. If such company transfers personal data to the US, it will also have to apply the Safe Harbor to the data transferred.

Transparency

- The categories of organizations that cannot participate in the Safe Harbor since they are not subject to the jurisdiction of the US Federal Trade Commission or the Department of Transportation should be more highlighted. In the current version of the Safe Harbor decision, such information is displayed in Annex III "Safe Harbor Enforcement Overview" amongst other detailed information. A solution could be the addition of a brief description of such categories in

[1] E.g., FAQ 6, 4th indent, provides for that self-certified organisations shall state in their privacy policy statements that they adhere to the Safe Harbor Principles, while it is not required in the "Notice" Principle. See also FAQ 7 which states that "assuring compliance with the Principles" as provided for in the "Enforcement" Principle implies the implementation of audits and training of employees, whereas not specified in the "Enforcement" Principle itself. See also FAQ 9.2 which provides for some exemptions to the "Choice" Principle that are not listed in the Principle itself. See also FAQ 12 which states that individuals should be able to opt out to direct marketing at any time, while opt-out is limited to disclosure to a third party controller and use of data for another purpose incompatible with the original one in the "Choice" Principle.

Annex I "Safe Harbor Privacy Principles", for instance as a footnote in the 3rd indent, and keep the more detailed content of Annex III.

- The scope of Safe Harborite's certifications that are available on the Department of Commerce's website should be made clearer. Indeed, many certificates give little information on their material scope and only specify whether it covers "offline", "on-line" and/or "manually processed" data, which does not give a clear indication of the categories of data that are covered (e.g. HR, customer's data and website users). In addition, whereas some organizations specify that their certificate covers all entities of the group, most organizations do not specify which legal entities are part of the group and thus that are covered by the Safe Harbor certificate.

- Self-certified organizations' privacy policies should be easily accessible[2] and understandable, especially concerning data subjects' rights. Privacy policies statements published on websites should be put forward in order to be easily found by data subjects, and designed in a clear way to allow data subjects understand what is done with their personal data and what are their rights. In this regard, the Department of Commerce could publish a set of guidelines on the drafting of Safe Harbor privacy policies and/or examples of Safe Harbor privacy policies, which could be developed in close cooperation with the European Data Protection Authorities, represented in the Article 29 Working Party.

- Data subjects should be clearly informed by self-certified organizations about their right to access their personal data and the means available to exercise it.

- A different list for those organizations who had participated to the Safe Harbor and whose certifications are no more valid could be envisaged. The introduction of the data of the beginning and the end of the Safe Harbor certification would also help keeping trace of those organizations which – even only for personal data collected during a short period of time – are bound by the Safe Harbor principles.

- The competences and roles of the Federal Trade Commission, the Department of Commerce, the DPA Panel and all the other institutions involved in the supervision and enforcement of the principles should be clarified, distinguished and more highlighted in order to prevent possible confusions.

- Certain key concepts in the Safe Harbor Agreement must be made clearer, such as "personal information", "aggregate data", "privacy program", "anonymous data", with a view towards the creation of a better understanding of the scope of application of the Safe Harbor in line with EU Directive.

Redress

- Data subjects should be granted the right to lodge a claim before a competent EU national court, in the same way as provided for in the other existing legal instruments designed for providing

[2] The WP29 supports the position of the DoC considering that a distinction could be made between the Privacy policies covering HR data that should be made accessible to the employees of the organisation and the Privacy policy covering personal information relating to individuals not part of the organisation (consumers, website visitors, clients, etc.), Indeed, 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).

safeguards in the context of data exports from the European Union to third countries[3]. Being able to bring claims for damages in the European Union concerning the processing of personal data constitutes a key requirement of effective data protection.

- Self-certified organizations should be prompted to choose alternative dispute resolution ("ADR") providers in the EU or the EU panel in order to comply with the fundamental rights to an effective remedy and to a fair trial[4]. To date, most ADR providers are based in the United States, which makes it harder for data subjects to introduce complaints with ADR providers, due to language and legislation differences, and cost and distance reasons. A solution might be to enable data subjects to lodge complaints to the EU panel in all cases.

- All ADR providers should possess the necessary tools to remedy situations of failure to abide by the Privacy Principles.

- In any case, data subjects should be entitled to issue a claim before their national data protection authority and this possibility should be explicitly foreseen in the Safe Harbor decision in order to clarify the role of the EU supervisory authorities. FTC should give priority to referrals of non-compliance with Safe Harbor principles from EU supervisory authorities as it is already foreseen in Annex V of the Safe Harbor decision for the benefit of Member States.

- In addition to rules on redress mechanism, there should be clearer rules on liability of Safe Harbor organizations towards data subjects.

Fees

- One of the main findings of the Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbor from the Perspective of EU Citizens and Companies Established in the EU from 27.11.2013 (COM (2013) 847) is that there are only very few complaints. Besides an improvement on the information of the data subjects about their rights this problem should also be addressed by creating an obligation for the Safe Harbor certified organizations to facilitate the data subjects' rights with the possibility to execute their rights free of charge.

Access by US authorities

- The ability to suspend transfers[5] should be clarified and the limitations to adherence to the Principles[6] should be restricted to minimize surveillance by submitting them to the EU proportionality and necessity principles[7]. Limitations to adherence to the Principles always entail the risk of breaching personal rights. Besides, additional safeguards should be introduced. The Commission should be notified by the Department of Commerce of any statute or government regulations that would affect adherence to the principle[8].

[3] E.g., any of the current EU Model Clauses enacted by the European Commission pursuant to Article 26 (4) of Directive 95/46/EC
[4] EU Charter of Fundamental Rights (Article 47); European Convention on Human Rights (Articles 6 and 13)
[5] Article 3 of the Safe Harbor Decision
[6] Annex I, Section 4 of the Safe Harbor Decision
[7] Directive 95/46/EC (Article 6 (1) (c) and 13); Treaty of the European Union (Article 5); EU Charter of Fundamental Rights (Article 52 (1))
[8] See WP32, p5.

- The EU definition of "data processing" should be added to the Safe Harbor Decision itself as the US concept of data processing does not include data acquisition, which means data protection rights are not applicable at this stage[9]. It has to be made clear in the Safe Harbor Decision that data acquisition is data collection and a form of data processing, which allows data subjects to exercise their rights already at this stage of data collection.

- Self-certified organizations should be allowed by national authorities to inform data subjects and competent DPAs of their surveillance and the Safe Harbor Decisions should contain an obligation to do so.

- EU data subjects should be granted with the same data protection rights than US ones, especially in case of surveillance through US national authorities.

Choice

The purpose specification principle of the EU Directive, also contained in the OECD Privacy Guidelines, is only partly replaced by a "choice" principle which in effect allows data collected for one purpose to be used for another, provided individuals have the possibility of opting out. The SH should comply with the purpose specification principle. Moreover, Choice should not be limited only to situations of disclosure to third party and to the use of data for incompatible purpose. This principle should be extended to cover all different use of personal data.

Access

- With regard to the right to access, it should be made clear that the person whose data are processed have access to all their processed personal data, not only to contact information or other specific data;

- Access principle provides for the right to have data deleted only in the case of inaccurate data and not where data is collected or processed without the data subject's consent or in a way that is incompatible with the principles. Access principle should be broaden to those situations;

- FAQ 8 introduces a long list of exceptions and the WP29 considers it too broad and limiting too much the individual rights in favour of the business interests.

Onward Transfer

- The WP29 considers it necessary to emphasize that this principle does not apply to the onward transfers outside of the United States if the onward transfers are known by the EU data Controller even before the transfer to the United States or if the EU data Controller is jointly responsible for the decision on onward transfers. In this case, in order to avoid any circumvention of the EU law, it should be made clear that the onward transfers should be considered as direct transfers from the EU to the third country outside of the US, and therefore articles 25 and 26 of Directive are applicable.

- According to the onward transfer principle, in order to disclose personal information to a third party, the organizations must apply the Notice and Choice principles. The WP29 considers that the further condition requiring that the third party provides at least the same level of privacy

[9] See Report on the Findings by the EU Co-chairs of the ad hoc EU-US Working Group on Data Protection, 27 November 2013, lit.3, p.9

protection as is required by the Safe Harbor principles should not be restricted to third parties acting as agents, but to any kind of third parties, also when acting as "data controllers". This is a fundamental principle to be considered in order to ensure that personal data continue to be protected adequately even after having been transferred onward.

- As regards to onward transfers to agents, the WP29 fully support the point of view of the COM stating that the Safe Harbor Decision should clarify the fact that agents receiving personal data for processing should be required to enter into a contract even if it is "Safe Harbor-compliant" or benefit from another adequacy finding solution[10].

- As regards to onward transfers to agents from self-certified organizations already acting as agents, it should be clearly stated that the contract signed with an EU controller (referred to in FAQ 10 "Article 17 contracts") determines whether an onward transfer is allowed. Therefore, if a self-certified organization is not explicitly allowed to do so by the EU controller, it cannot transfer the data to a subsequent agent.

- A self-certified organization deciding to onward transfer data should stay fully liable for the proper handling of the data. As a consequence, the last sentence of the "Onward transfers" Principle should be rephrased to specify that the main "processor" (agent) should remain liable towards the EU controller. When the self-certified organization is acting as a controller and transfers onward the data to a third party, it should remain liable to the data subjects.

Security

- Self-certified organizations should have the obligation to implement technical and organizational measures that are "appropriate to the state of the art and the risks represented by the processing and the nature of the data to be protected" instead of only taking "reasonable precautions".

Applicability to agents/processors in the US (FAQ 10)

- The rules of applicability of the Principles to self-certified organizations receiving data from the EU merely for processing (agent or "processor") should be clarified as the current content of FAQ 10 is confusing and unclear on the question whether a self-certified organization acting as "processor" (agent) has to apply the Principles. Furthermore, if they are actually exempted from such adherence, the explanation provided in FAQ 10 is questionable insofar as it relies on the fact the EU controller remains responsible of the personal data sent to such "processor" (agent) vis-à-vis data subjects. Finally, considering their importance, a specific principle dedicated to processors/agents should be included in the Safe Harbor to clarify the applicable rules.

Human resources (FAQ 9)

- The statement according to which pseudonymized data does not raise privacy concerns[11] should be modified to match with the EU notion of "personal data"[12] according to which personal data is defined as any information relating to an identifiable natural person. Consequently,

[10] It is a question of clarification in the Decision since on substance, the DoC agrees on the principle, See: "Clarifications Regarding the U.S.-EU Safe Harbor Framework and Cloud Computing":http://export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf

[11] FAQ 9, answer to question 1

[12] Directive 95/46/EC (Article 2 (a))

pseudonymized data most certainly can be a case of information relating to an identifiable natural person.

- The limitation to providing notice and choice to employees where necessary to safeguard the legitimate interests of the organization in making promotions, appointments, or other similar employment decisions[13] should be restricted. It is questionable in cases of a decision concerning employment that this exception could not be applied to.

Publicly available information (FAQ 15)

- The exemption for publicly available and public record data is not in line with the EU Directive. Moreover the exemption of liability for such information should be removed.

Principle of proportionality or reasonableness

- A processing of personal data could, even under a strict respect of Notice and Choice, be not proportionate with regards to the interests' rights and freedoms of the data subject or society. The principle of proportionality or reasonableness is to be respected at all stages of the processing and should be applicable **in addition** to the principles of Notice and Choice.

- Transparency towards individuals and the possibility for her/him to express its will are fundamental but cannot override the necessity for the processing to be proportionate.

- What is to be considered a legitimate purpose depends on the circumstances as it aims to ensure that a balancing of all rights, freedoms and interests at stake is made in each instance; the right to the protection of personal data on the one hand, and the protection of other rights on the other hand, as, for example, between the interests of the data subject and the interests of the controller or of society.

Accountability

- The Working party would consider useful to include all the existing "accountability" duties within a specific principle dedicated to Accountability (see for instance, the reference to internal complaint mechanism, external or internal reviews of compliance, training of employees, corporate officer or other similar function in current FAQ 7). It could help to clarify the internal measures needed to be implemented within the self-certified organizations.

[13] FAQ 9, answer to question 2, last indent