

ARTICLE 29 Data Protection Working Party



Brussels, 05 February 2015

Ms Věra Jourová
Commissioner for Justice, Consumers and
Gender Equality
European Commission
By E-mail:

Dear Ms Jourová

Following the previous exchanges with the European Commission concerning the consequences of US surveillance programmes involving massive, indiscriminate and disproportionate collection and processing of personal data, including data originating from the European Union, the Article 29 Working Party would like to draw your attention to the following additional considerations.

The Working Party has already stated in its opinion adopted on 10 April 2014 that massive, indiscriminate and disproportionate access by US authorities to data originating from the EU cannot be considered to be in line with the Safe Harbour Principles and its possible limitations.¹ According to the Safe Harbour Decision and to the Court of Justice of the European Union's settled case-law, derogations and limitations in relation to the protection of personal data must apply only in so far as is strictly necessary and must not be used in a way that undermines the protection afforded by the Principles.² It follows from these elements that we have serious concerns about the proper implementation of the Safe Harbour arrangement.

In this respect, the Commission already considered that "*the large scale access by intelligence agencies to data transferred to the US by Safe Harbour certified companies raises [...] serious questions regarding the continuity of data protection rights of Europeans when their data is transferred to the US*"³. Therefore it identified a number of recommendations among which two concerned the access to data by US authorities which are currently discussed with the US authorities.

While the Working Party fully supports all the recommendations made by the Commission, and in particular Recommendations 12 and 13 relating to access by US authorities, it also considers that it is of the utmost importance that the Working Party's additional recommendations, including on the access by US authorities, sent to Vice-President Viviane Reding on 10 April 2014, are also implemented. Therefore, in the light of the ongoing negotiations, the Working Party stresses the need to ensure that "the limitation to adherence to the Principles should be restricted to minimize

¹ Article 29 Working Party, Opinion 04/2014 on Surveillance of electronic communications for intelligence and national security purposes, - WP 215

² See footnote 1 and Case C 473/12, §39

³ European Commission, COM(2013) 847 on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, p. 18

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Fundamental rights and Union citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No MO59 02/34

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

surveillance by submitting them to the EU proportionality and necessity principles” and that “EU data subjects should be granted with the same data protection rights than US ones, especially in case of surveillance through US national authorities” (see ANNEX I).⁴

The Working Party furthermore stated 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 and recalled that, in any case, data protection authorities may suspend data flows according to their national competence and EU law.

While the Working Party welcomes the negotiations on the Safe Harbour Decision, it recalls that transfers made on the basis of this Decision are not the only transfer tools affected by the recent surveillance revelations since those made by Edward Snowden.⁵ While the Commission is already addressing exclusively Safe Harbour, there are solutions to be found for the other transfer instruments too (i.e. Standard Contractual Clauses and Binding Corporate Rules).

In that respect, the rules in terms of notification to data protection authorities regarding foreign judicial and administrative requests to access data should be clarified. This question is especially relevant in the context of the European Parliament proposed Article 43a of the draft Regulation.

EU data protection authorities consider that a coherent and comprehensive answer to the issue of massive, indiscriminate and disproportionate surveillance by foreign authorities should be urgently provided in line with the requirements of the Directive 95/46/EC and EU case-law principles of necessity and proportionality.

Finally, the Working Party considers that trust can only be restored through the negotiation of an international agreement providing adequate protection against indiscriminate surveillance. This agreement shall include obligations on the necessary oversight of surveillance programmes, on transparency, on redress mechanisms and data protection rights.

The Working Party and EU DPAs will further reflect on potential solutions for these issues and remain available for any further input.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN
Chairwoman

⁴ Letter from the Article 29 Working Party to Vice-President Viviane Reding on the actions set out by the European Commission in order to restore trust in data flows between the EU and the US, see ANNEX I.

⁵ In fact, the Working Party recalls that “none of the instruments available that can be used as an alternative basis to transfer personal data to countries that have not been found adequate (Safe Harbor, Standard Contractual Clauses and BCRs) allow for third country public authorities for the purpose of indiscriminate, massive surveillance to gain access to personal data transferred on the basis of these instruments” (Article 29 Working Party, Opinion 04/2014 on Surveillance of electronic communications for intelligence and national security purposes, - WP 215).