

## ARTICLE 29 Data Protection Working Party



Brussels, 08 September 2015

Mr Dimitris Avramopoulos  
Commissioner  
Migration, Home Affairs and Citizenship  
B-1049 Brussels

Mr Christian Braun  
Ambassador Extraordinary and Plenipotentiary  
Permanent Representative  
Avenue de Cortenbergh 75  
1000 Brussels, Belgium

Mr Claude Moraes  
Chair of the Committee on Civil  
Liberties, Justice and Home  
Affairs  
European Parliament  
Rue Wiertz 60  
1047 Brussels

Subject: Letter on the European Agenda on Security

Dear Mr Avramopoulos,

Dear Mr Moraes,

Dear Mr Braun,

After the Paris attacks, the European data protection authorities assembled in the Article 29 Working Party (hereafter “the WP29”) reiterated their collective commitment to contribute to preserving European values and principles and, in particular, to the necessity of ensuring that an appropriate balance is struck between public security requirements and the right to the protection of private life and of personal data. It insisted that these objectives, although different, are not contradictory objectives.

It is with this perspective in mind that the WP29 carefully read the Commission’s Communication on the European Agenda on Security (here after “the Communication”) and would like to share the comments that emerged in the course of its analysis.

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 for Justice and Consumers, B-1049 Brussels, Belgium, Office No MO59 02/34

Website: [http://ec.europa.eu/justice\\_home/fsj/privacy/index\\_en.htm](http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm)

First of all, the WP29 welcomes the strong message given to all stakeholders and citizens involved in the legislative process that any new legislative proposal needs to be compliant with fundamental rights in general and with the right to data protection and the right to privacy in particular, as enshrined in Article 7 and 8 of the Charter of Fundamental Rights and in Article 8 of the European Convention on Human Rights. WP29 believes that respect for fundamental rights (including rights to respect for private life and to data protection) should be an integral part of every aspect of JHA policy. It notes that a large number of the policy measures announced in the Communication will involve the processing of personal data: smart borders, PNR schemes, the reinforcement of Europol tasks, ECRIS, EPRIS, mutual legal assistance treaties, the fight against cybercrime, Prüm and SIS II.

In this regard, the WP29 notes that there is still room for finding a better balance between the fight against threats to public security and the effective application of data protection rules.

To this end, in its opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211), the WP29 explains the need to undertake necessity and proportionality tests before proposing any new legislative act. This is all the more important in the light of the CJEU data retention judgment. The opinion also recalls the obligation to pursue a legitimate aim and ensure that the scope of the proposal is limited to the strictly necessary, to introduce measures to safeguards fundamental rights according to Art. 52 (1) of the Charter of Fundamental Rights and the need to review existing measures and alternatives to show why existing measures are no longer sufficient for meeting the primary/original need.

The WP29 supports the view that existing legal instruments should be used to their full potential before any new instrument is created. According to the draft manual on law enforcement information exchange (doc. number 7779/15)<sup>1</sup>, there are twelve different European channels of information exchange and ten European information systems used by law enforcement authorities from Member States for the purpose of preventing and combating crime, fighting terrorist offences and maintaining public order. In line with the concerns expressed in the Communication, the experience of the DPAs assembled within the WP29 is that some of these instruments are not fully implemented and used by Member States (amongst others the Prüm Decision), and therefore cannot be fully effective. Law enforcement agencies already have access to and process large amounts of personal data, and in consequence, more data subjects are becoming concerned by such processing. Therefore the

---

<sup>1</sup>See document available on Statewatch website: <http://www.statewatch.org/news/2015/may/eu-council-manual-law-enforcement-information-exchange-7779-15.pdf>

WP29 is of the opinion that need to introduce new instruments proposed in the European Agenda on Security should be carefully evaluated.

Once these necessity and proportionality tests have been performed, the WP29 reminds that any new instrument should include specific measures implementing data protection requirements of fair and lawful data processing, purpose limitation, data minimization, privacy by design and data retention, and that all the principles should be promoted amongst law enforcement authorities to enable the application of fundamental rights.

The WP29 draws the attention of the EU legislator to its opinions WP 145 on the use of Passenger Name Record (PNR) for law enforcement purposes<sup>2</sup>, WP 178 on the global approach to transfers of Passenger Name Record (PNR) data to third countries<sup>3</sup>, and WP 206 on Smart Borders<sup>4</sup>, which apply this reasoning to specific measures mentioned in the Communication. It also refers to its letters addressed to the Cybercrime committee of the Council of Europe with regard to the data protection implications of transborder access to data in the context of cybercrime.<sup>5</sup>

The WP insists that this data protection compliant approach should also apply to less formal actions or documents such as action plans, strategies or best practices codes.

The WP29 highlights that those principles will remain at the forefront of the new Data Protection Package and, more specifically, in the Data Protection Directive. In this regard, it remains crucial for the trilogue process for the new Data Protection Package (Regulation *and* Directive) to be completed as soon as possible, which would guarantee a minimum common standard of data protection for law enforcement authorities of all Member States. There is also a need to develop/have one, common, or at least similar, high level of data protection and data protection oversight/supervision in all JHA instruments.

Taking into account the emphasis the Commission places on compliance with fundamental rights and, in particular, data protection, the WP29 will closely follow the different matters addressed in the Communication, and would appreciate being involved, when and where relevant, in the debate. This engagement would be a good starting point for our future cooperation concerning new initiatives in the JHA area, especially those deriving from the

---

<sup>2</sup> [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp145_en.pdf)

<sup>3</sup> [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp178\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp178_en.pdf)

<sup>4</sup> [http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206\\_en.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp206_en.pdf)

<sup>5</sup> See letter of the WP29 dated 28 November 2014 available at [http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20141128\\_\\_letter\\_of\\_the\\_art\\_29\\_wp\\_t-cy\\_on\\_the\\_cybercrime\\_scenarios\\_\\_not\\_signed.pdf](http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2014/20141128__letter_of_the_art_29_wp_t-cy_on_the_cybercrime_scenarios__not_signed.pdf)

European Agenda on Security. Additionally, for the same reason, the WP29 would be happy to share its data protection expertise by participating in the EU Security Consultative Forum.

We remain at your disposal for any questions you may have on these subjects.

Yours sincerely,

On behalf of the Article 29 Working Party,

Isabelle FALQUE-PIERROTIN  
Chairwoman

CC: MsVěra Jourová, Commissioner Justice, Consumers and Gender Equality  
Mr Martin Schulz, President of the European Parliament