

## ARTICLE 29 Data Protection Working Party

Paris, 30 June 2014  
Lara Ballard  
Special Advisor for Privacy and  
Technology  
U.S. Department of State  
National Telecommunications and  
Information Administration  
1401 Constitution Ave.  
NW Washington, DC 20230

By email: BallardLA@state.gov

Dear Ms Ballard,

Pursuant to your solicitation concerning the public inquiry regarding “big data” and the Consumer Privacy Bill of Rights, I wish to share with you some elements relating to the position of the Article 29 Working Party on big data.

Indeed, big data raises important concerns regarding the privacy of the individuals concerned and the protection of their rights.

In that respect, the WP29 has recently examined the issue of the risk based approach which is highly relevant in the context of big data. The corresponding statement adopted by the Working Party is joined (see the document attached).

You will also find attached the letter which has been sent to Mr Podesta following the publication of the report “Big data: seizing opportunities, preserving values” in May. The WP29 is currently working on the adoption of a statement to publish its general position on these matters. We shall send you this document as soon as it is released.

The WP29 hopes that you will find these elements useful.

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

Yours sincerely,



Isabelle FALQUE-PIERROTIN  
Chairwoman



**14/EN  
WP 218**

**Statement on the role of a risk-based approach in data protection legal frameworks**

**Adopted on 30 May 2014**

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, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

## Statement of the WP29 on the role of a risk-based approach in data protection legal frameworks

The Article 29 Working Party (WP29) has always supported the inclusion of a risk – based approach in the EU data protection legal framework. In particular, its statement of 27 February 2013 on current discussions regarding the data protection reform package contained the following specific reference to the risk-based approach:

*“The Working Party recognizes that some of the provisions in the proposed Regulation may pose a burden on some controllers which may be perceived as unbalanced and has therefore in earlier opinions already expressed the view that all obligations must be scalable to the controller and the processing operations concerned. Compliance should never be a box-ticking exercise, but should really be about ensuring that personal data is sufficiently protected. How this is done, may differ per controller..... Data subjects should have the same level of protection, regardless of the size of the organisation or the amount of data it processes. Therefore the Working Party feels that all controllers must act in compliance with the law, though this can be done on in a scalable manner.”*

Despite this, the Working Party is concerned that both in relation to discussions on the new EU legal framework for data protection and more widely, the risk-based approach is being increasingly and wrongly presented as an alternative to well-established data protection rights and principles, rather than as a scalable and proportionate approach to compliance. The purpose of this statement is to set the record straight.

The so-called “risk-based approach” is not a new concept, since it is already well known under the current Directive 95/46/EC especially in the security (Article 17) and the DPA prior checking obligations (Article 20). The legal regime applicable to the processing of special categories of data (Article 8) can also be considered as the application of a risk-based approach: strengthened obligations result from processing which is considered risky for the persons concerned. It is important to note that – even with the adoption of a risk-based approach – there is no question of the rights of individuals being weakened in respect of their personal data. Those rights must be just as strong even if the processing in question is relatively ‘low risk’. Rather, the scalability of legal obligations based on risk addresses compliance mechanisms. This means that a data controller whose processing is relatively low risk may not have to do as much to comply with its legal obligations as a data controller whose processing is high-risk.

However, the risk-based approach has gained much more attention in the discussions at the European Parliament and at the Council on the proposed General Data Protection Regulation. It has been introduced recently as a core element of the accountability principle itself (Article 22). In addition to the obligation of security (Article 30) and the obligation to carry out an impact assessment (Article 33) already prescribed in the draft regulation, the risk-based approach has been extended and reflected in other implementation measures such as the *data protection by design* principle (Article 23), the obligation for documentation (Article 28) and the use of certification and codes of conduct (Articles 38 and 39). It is apparent therefore that the draft Regulation already contains the tools – for example in Article 33 relating to impact assessment – to provide for a reliable and relatively objective assessment of risk.

In parallel, the concept has been promoted in public debates on data protection regulation in the context of “big data”. Its promoters argue that *collection* should no longer be considered

the main focus of regulation and that legal compliance should rather shift to the framing of data *use*. To comply, it is advocated that a strong harm-based approach can help to promote responsible data use based on risk management.

Finally, there have been vigorous debates at the European Parliament and at the Council on the applicability of a lighter legal regime for pseudonymous or pseudonymised data considering that because of their perceived less identifiable nature, the privacy risks for data subjects are reduced.

Those contextual and background elements show the compelling need for the Working Party to communicate the following key messages on this issue.

\*\*\*\*

1/ Protection of personal data is a fundamental right according to Article 8 of the Charter of Fundamental Rights. Any processing operation, from collection to use and disclosure, should respect this key right.

2/ Rights granted to the data subject by EU law should be respected regardless of the level of the risks which the latter incur through the data processing involved (e.g. right of access, rectification, erasure, objection, transparency, right to be forgotten, right to data portability).

3/ There can be different levels of accountability obligations depending on the risk posed by the processing in question. However controllers should always be accountable for compliance with data protection obligations including demonstrating compliance regarding any data processing whatever the nature, scope, context, purposes of the processing and the risks for data subjects are.

4/ Fundamental principles applicable to the controllers (i.e. legitimacy, data minimization, purpose limitation, transparency, data integrity, data accuracy) should remain the same, whatever the processing and the risks for the data subjects. However, due regard to the nature and scope of such processing have always been an integral part of the application of those principles, so that they are inherently scalable<sup>1</sup>.

5/ Implementation of controllers' obligations through accountability tools and measures (e.g. impact assessment, data protection by design, data breach notification, security measures, certifications) can and should be varied according to the type of processing and the privacy risks for data subjects. There should be recognition that not every accountability obligation is necessary in every case – for example where processing is small-scale, simple and low-risk.

6/ The form of documentation of the processing activities can differ according to the risk posed by the processing. Yet, all data controllers should at least to some extent document their processing activities in order to further transparency and accountability. Documentation is an indispensable internal tool for controllers to manage accountability effectively and for ex-post control by DPAs as well as for the exercise of rights by data subjects. It goes beyond information to be given to the data subjects.

---

<sup>1</sup> See e.g. the use of "adequate", "appropriate", "reasonable" and "necessary" in Articles 6 and 7 of Directive 95/46/EC

7/ Risks, which are related to potential negative impact on the data subject's rights, freedoms and interests, should be determined taking into consideration specific objective criteria such as the nature of personal data (e.g. sensitive or not), the category of data subject (e.g. minor or not), the number of data subjects affected, and the purpose of the processing. The severity and the likelihood of the impacts on rights and freedoms of the data subject constitute elements to take into consideration to evaluate the risks for individual's privacy. The proposed Regulation – for example Article 33 – already contains the criteria needed to assess the privacy risk posed by particular processing.

8/ In the context referred to above, the scope of “the rights and freedoms” of the data subjects primarily concerns the right to privacy but may also involve other fundamental rights such as freedom of speech, freedom of thought, freedom of movement, prohibition of discrimination, right to liberty, conscience and religion.

9/ The risk-based approach requires additional measures when specific risks are identified (e.g. impact assessment, enhanced security, data breach notification) and the DPA should be consulted when highly risky processing has been identified by an impact assessment (Article 34 of the draft regulation).

10/ In its statement of 27 February 2013, the Working Party recalled that data protection rules continue to apply to pseudonymous or encrypted data where it is possible to backtrack an individual or (indirectly) identify an individual by other means (see statement, page 1). Yet, it also acknowledged that using pseudonymising techniques to disguise identities to enable collecting data relating to the same individual without having to know his/her identity can help reduce the risks to individuals. These techniques thus represent important safeguards, which can be taken into account when assessing compliance. Nevertheless, the use of pseudonymous or pseudonymized data is, in itself, not sufficient to justify a lighter regime on accountability obligations.

11/ The risk-based approach goes beyond a narrow “harm-based-approach” that concentrates only on damage and should take into consideration every potential as well as actual adverse effect, assessed on a very wide scale ranging from an impact on the person concerned by the processing in question to a general societal impact (e.g. loss of social trust).

12/ The legitimate interest pursued by the controller or a third party is not relevant to the assessment of the risks for the data subjects. It is in applying the balancing test under the criteria for making the data processing legitimate under the Directive (Article 7 f.) or of the draft regulation (Article 6 f.) that the legitimate interest should be taken into account.

13/ Under the forthcoming regulation, the DPAs' role with respect to the risk-based approach will namely consist of:

- updating the list of processing which can be considered to present specific risks by essence (Article 33 of the draft regulation),
- developing guidelines on impact assessments and on other accountability tools (as the CNIL and the ICO did with their privacy risk management methodology),
- carrying out enforcement procedures in case of non compliance of controllers, which may imply challenging risk analysis, impact assessments as well as any other measures carried out by data controllers,
- targeting compliance action and enforcement activity on areas of greatest risk.

## ARTICLE 29 Data Protection Working Party



Brussels, 11 June 2014

Mr John PODESTA  
Counselor to the President  
The White House  
1600 Pennsylvania Avenue NW  
WASHINGTON, DC 20500  
UNITED STATES OF AMERICA

E-mail: [jpodesta@who.eop.gov](mailto:jpodesta@who.eop.gov)

Dear Mr Podesta,

I am writing to you in my capacity of Chair of the Article 29 Working Party, the EU independent advisory body on data protection and privacy set up under Article 29 of the Data Protection Directive 95/46/EC.

The Working Party has read with great interest the report “Big data: seizing opportunities, preserving values” which was released by your office last month. The report devotes substantial attention to the privacy issues raised by the development of big data, which naturally coincides with the Working Party’s own concerns and work.

The Working Party welcomes a number of policy recommendations made in the report, namely the extension of privacy protections existing in the United States to non-US persons. The effectiveness of such an extension is indeed critical for European citizens in the aftermath of the recent revelations on the mass surveillance programmes operated on European citizens by intelligence services, notably in the United States.

Also, the Working Party takes note of your support for the greater interoperability of privacy standards at the international level, which it also considers as a key element to ensure the effective protection of individuals with regard to the processing of their personal data, in the EU and elsewhere.

It also agrees with the idea that processing techniques applied to big data could lead to discriminatory outcomes, infringing the right to equal treatment and to not be discriminated.

For all these reasons, the Working Party looks forward to contributing to the transatlantic cooperation on the practical follow-up of these proposed measures, so that EU as well as US concerns are duly taken into consideration.

Many important benefits are expected from the development of big data. Nevertheless, big data also raises important concerns with regard to the privacy of the individuals concerned, the civil rights protection, as well as social and ethical questions.

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, B-1049 Brussels, Belgium, Office No MO-59 02/013.

Website: [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm)

An appropriate balance must be struck between these expected collective benefits and the risks for individuals. This naturally raises the question of whether this balance can be struck within the existing legal framework that is applicable to the development of this trend.

Directive 95/46/EC and other relevant EU legal instruments are clearly part of this framework, as most of the big data trend entails the extensive processing of data on EU citizens.

Their relevance is even greater since the landmark ruling of the European Court of Justice of 13 May 2014 in the Google Spain case, which makes it necessary to take EU data protection rules into account when assessing the impact of the advertising-supported ecosystem on the Internet on the protection of individuals with regard to the processing of their data.

Some stakeholders tend to believe that the basic data protection principles and obligations require accommodation to enable promising forthcoming developments in big data to take place.

At this stage, the Working Party has no reason to believe that the EU data protection principles, as they are principally enshrined in Directive 95/46/EC, are fundamentally challenged by the development of big data.

In fact, as your report clearly shows, big data is a broad term that covers a great number of data management cases, some of which are already well-identified, some of which are only partially apprehended and even unclear. A number of the cases identified in the report – such as the development of comprehensive information systems in the delivery of health services or in the centralisation of law enforcement files – also exist in the EU Member States that could be adequately framed by existing European data protection rules, whether at EU- or national levels.

On the basis of these shared national experiences, the Working Party recently released a number of policy documents, which it believes are consistent with the analysis of some privacy concerns which are identified in the report – e.g. its Opinion 05/2014 on Anonymisation Techniques or its Opinion 01/2014 on the Application of necessity and proportionality concepts and data protection within the law enforcement sector. In this context, the Working Party also refers to its Opinion 03/2013 on purpose limitation, its Opinion 06/2013 on open data and public sector information re-use, and its Opinion 06/2014 on legitimate interest.

With all these elements in mind, the Working Party intends to carry out its own assessment of the development of big data on the basis of the EU legal framework.

The Working Party looks forward to further exchanges on these fascinating developments in the near future, in particular on the proposition that relates to the protection of EU citizens.

Yours sincerely,

On behalf of the Article 29 Data Protection Working Party,

Isabelle FALQUE-PIERROTIN

Chair

Cc:

- Ms Viviane Reding, Vice-President, European Commission
- Ms Penny Pritzker, US Secretary of Commerce
- Mr. Ernest J. Moniz, US Secretary of Energy
- Mr. John HOLDREN, Director, Office of Science and Technology Policy
- Mr. Jeffrey ZIENTS, Director, US National Economic Council