



## **The EU Data Protection Reform: Updated Perspectives and the Challenges posed by Big Data**

Istanbul, 21 May 2014

*Giovanni Buttarelli*  
*Assistant European Data Protection Supervisor*

Speaking points at Inet Istanbul. Internet: Privacy and Digital Content in a Global Context

### **1) The EU Data Protection Reform: a short update.**

Two and a half years after the European Commission launched the review of the European Data Protection legislation, the EU package, though not in difficult waters, is still in motion towards a 'Safe Harbour'.

At the EDPS, we are very grateful to the European Parliament for the strong stance it took, when, in the March Plenary, it voted to adopt a compromise text on such a difficult issue. The package represents one of the most important dossiers of the current legislative term, as the heavy lobbying which surrounded it and the 3999 amendments clearly showed.

Where are we now, in terms of the legislative process?

The Parliament is ready to start the relevant negotiations within trilogues while in Council, EU Member States are working to agree on a common position - building on the partial agreement achieved under the Irish Presidency and the subsequent commitment to reach an agreement expressed by the European Council in October last year, when concerns about surveillance programmes peaked worldwide.

A Member States agreement could be achieved at the next JHA Council on June 5 and 6, but a global one may perhaps require more time and only be formalised under the Italian Presidency. Indeed, discussions on Chapter V seem to be very advanced, whilst other issues may require few other discussion, such as those relating to profiling, the obligations of controllers and processors, the risk based approach and, of course, the one-stop-shop mechanism.

As EDPS, we continue to firmly support the Reform and agree on its main points, regardless of some clarifications and adjustments that may be needed in the final rush to facilitate the agreement.

Timing remains key for the Reform, but substance is more important. That's why I would like to spend my time with you today sharing some concerns about data protection and Big Data rather than simply celebrating the importance of a new, harmonised legislation, which as you know will be applied horizontally across all controllers around the world, offering goods and services to EU residents or monitoring their behaviour.

Indeed, the choices made by the EU will be influential everywhere around the world, though only few of the 20 Big Data players are currently based in the European Union.

Let me select two main questions only for today's debate.

The first is the following:

**2) How much modern and flexible is the Data Protection Reform to cope with the challenges posed by Big Data?**

Big Data is not only a data protection issue.

However, analysis from a privacy and data protection viewpoint should not be marginalised.

Indeed, the pace and impact of technological innovation has led to an age of Big Data and this has profound implications for society.

Without going into the various definitions of Big Data, let me just say that most of them highlight the growing capability of new software and hardware devices to capture, transfer, merge and extrapolate potentially unlimited volumes of information, in multiple ways and faster than ever. It will soon become difficult to process this data by using standard management tools or traditional processing operations.

What, then, is the right approach to take from a data protection perspective?

The explosion of more or less reliable information will once again change the way we live. Big Data collection and analysis can undoubtedly improve our societies. Where used well, it may help to generate prosperity and improve well-being. Where not used irresponsibly also for discrimination or surveillance, Big Data may offer clear prospects for significant benefits for, citizens, consumers, governments and businesses.

But what about the increased risks Big Data poses to the fundamental rights of individuals?

On the basis of a solid legal background, including the Lisbon Treaty and the Charter of Fundamental Rights, individuals in the EU will continue to be adequately protected, also by the fundamental right to only be subjected to the processing of personal data when it is fair, performed for specified and transparent purposes, on the basis of the consent of the person concerned or some other legitimate basis laid down by law and, finally, provided that compliance is subject to control by an independent authority. We hope that a US Consumer Privacy Bill of Rights will soon introduce robust safeguards in an interoperable way.

However, even when well used, Big Data may skew the amount of information collected.

Indeed, social media, apps, and apparently free-of-charge online products and services are already designed to maximise the amount of information to be collected and analysed, using it as an incentive to attract investors as well as to maximise their return on advertising.

The G8's 2013 Open Data Charter highlights a principle of *'open by default'*, to make data more freely and openly re-usable.

Finally, in this era of the 'Internet of Things', which builds among others on our domestic devices, vehicles and sensors embedded through wearable techniques, costs to collect, share and store information will be driven down.

Then:

-are the modern rules we're now introducing in Europe sufficiently global, flexible and technology-proof to be effective?;

-in the new world of Big Data, how better will users and consumers be informed on how their data will be used and by whom? And if they are informed, will such privacy statements be easily understood?;

-how in control will those that provide data, intentionally or inadvertently, hundreds of times, be of the multiple ways in which this data is tracked and profiled?

### **3) Is Big Data really so challenging for Data Protection?**

These questions can be answered with more questions!

For instance, is Big Data truly an entirely new data protection challenge, compared to what we have tested in previous generations of data protection rules, when moving from manual to automated processing, from analogic to digital networks, from the pioneering development of e-commerce to the Information Society, from the silos to interconnected large-scale data systems?

It can be argued that the volumes of Big Data, new high-performance computing, sophisticated technologies and the patterns, correlations, relationship and results achievable with such an explosion of information are and will be unprecedented.

Not only will there be huge amounts of completely new and gigantic datasets, but also new methods and algorithms to analyse and use them.

More opportunities and risks will operate for controllers and data subjects immediately after data fusions, largely in real-time or instantly after data is captured. Users and consumers may soon be overwhelmed by the increased level of sophistication and the pervasiveness of predictive and real-time large scale software.

I'm sure you agree on the need to reinforce existing safeguards against profiling and other software that can predict human behaviours and preferences. I'm sure you also agree on the need for balance between the creation of previously unthinkable ways to profile the moments of the daily life of users and citizens, to combat price discrimination, among other things, or access to information and services. The same notion of harm concerning users and consumers may perhaps will require continuous attention.

Not all Big Data information will include personal data. However, the value of dispersed data will change and increase a lot. As a consequence, an increasingly larger part of data sets will include personal data concerning directly or indirectly identifiable individuals.

Therefore, the concept of identifiability will require constant monitoring to verify what new computational capabilities will allow on the basis of unstructured sets of data amassed for different purposes and in different contexts. Technologies aiming to re-identify individuals will evolve constantly in a way which is still unpredictable. Re-identification techniques will make it extremely easy to combine small pieces of non-identifiable data, leading to a sort of mosaic or puzzle effect, possibly unintentionally in cases where the controllers were not committed to identify/re-identify individuals. Although this will be possible even in cases where personal identifiers are not used, users would be entitled to have a say over their use.

Moreover, new challenges to the quality of data requirements are to be expected, since the information revealed by Big Data is not necessarily reliable, accurate and therefore trustworthy. For instance, human error or interpretation, particularly in the case of automated decisions affecting individuals, will sometimes remain determining factors.

Big Data may also represent a new challenge for other data protection pillars, including the need-to-know and the purpose limitation principles (just think of the many

different categories of data collected in different areas, by different players and in very separate contexts: who will be considered controller for what?)

It is also clear that current data retention time limits will be again challenged, since more and more data will be generated constantly and could be easily preserved beyond the current proportionate time limits.

Finally, I am not overstating when I say that Big Data also means elaboration of aggregated information concerning multiple clusters of individuals categorised or strictly interlinked with each other in a group of friends, relatives, professionals or users. New segments and relationships will be created and as is the case for genetic data in some cases we may have co-data subjects.

#### **4) Conclusions.**

When Convention 108 and the first OECD Guidelines were drafted, people wanted a better understanding of the principles for the proper use of computers.

Both these legal instruments have in some way survived the ravages of time, offering continuity together with Directive 95/46/EC even after the revision of the OECD Guidelines and in the course of the modernisation of the Convention 108.

You may raise the question of whether our contemporary rules, particularly those we expect to become law within a year from now, will be modern, flexible, robust and effective enough to protect our fundamental rights and freedoms.

It will not be easy to have immediately all the answers and satisfy all needs, from a data protection perspective, to the discoveries, innovation, opportunities and risks that Big Data still presents.

However, my sense is that the current EU package may help a great deal with the new challenges, provided we take a proactive and flexible approach both in terms of content and implementation. And, when I say flexible I do not mean lowering safeguards but rather avoiding useless details that may not resist to the rapid developments of technologies.

In sum, the EU Data Protection Reform is the robust and right approach we need even in front of Big Data.

Recent European Court of Justice's judgments on Google Spain and on retention of traffic data cases support this assumption when focusing on the scope of data subject's rights guaranteed by Directive 95/46/EC or, respectively, the retention of data as a particularly serious interference with fundamental rights.

At the EDPS, with our preliminary Opinion on competitiveness in the age of Big Data, adopted in April, we have launched a discussion between policymakers, regulators and experts, with a view to exploring new specific interactions with consumer law.

In conclusion, discussions should continue on how to better balance Big Data and its social and ethical implications, on how to constantly implement our data protection strategies to ensure that we are not surprised by rapid developments, so that new checks and balances are ready in response to those developments.

A robust data protection framework is an essential pre-condition for our increasingly data-driven society.

In short, as rightly stated in the White House 90-day study released on May 1, Big Data -used well- can be used to change the world positively without changing citizens' belief in the value of protecting our rights.

-----