Value of the EU Data Protection Reform against the Big Data challenges

Keynote address
5th European Data Protection Days
Berlin, 4.5.2015

Giovanni Buttarelli
European Data Protection Supervisor

(Check Against Delivery)

Ladies and gentlemen,

It is an honour to be here today. I would like to share with you what I believe to be some of the biggest choices facing Europe. Choices which are facing other parts of the world, as Julie Brill has just explained.

I would like to thank the organisers for their invitation and I would especially like to thank Julie for her pragmatic and comprehensive résumé of the latest developments in the US on the protection of privacy.

Let me start with a message that I hope will resonate with all of you:

We need global bridges to be able to protect the personal data and privacy of the individuals facing borderless technologies, business models and networks that use their data as fuel.

What Julie and I have in common is a passionate commitment to building bridges for privacy protection. Bridges which are secure and dependable, inwhich citizens and businesses in our democracies can have confidence.

The Safe Harbor agreement, regardless of the considerable, and in my view justified, criticism it receives, is a mutual attempt at bridging the divide. The EU-US umbrella agreement on data protection, still under negotiation, is another.

But if you look at the history of the most beautiful and strongest bridges in the world, you'll notice that their construction begins with solid pillars from both sides.

The US in its Constitution, and the EU in its Charter of Fundamental Rights, have each laid down the foundations of these pillars. The EU put it into law with the Data Protection Directive, now under revision.

An unambiguous and coherent Consumer Privacy Bill of Rights in the US would be the most powerful signal of reciprocity.

Just like the internet has connected the whole planet, so we need similar constructions which protect the interests of the individual between all regions, not just the US and Europe.

This common enterprise is more important and urgent that ever. We need solutions which focus on individuals as such, not only on users, consumers and subscribers.

So this morning I want to talk about the Big Data challenge for our societies and for individual freedom. Then, I will explore in depth the solutions I believe we can implement to meet these challenges, while benefitting from the advantages that Big Data can bring.

These solutions, I will argue, are fourfold:

1) they should stem from an ethical approach to developing technology and related business models;

2) they should stem from reformed legal rules;

3) they should encompass technical solutions, such as privacy by design, and

4) they should be implemented through enforcement cooperation.

Finally, I will share with you how the EDPS is putting these solutions into practice.

Our economies are globalised. We live in the Internet age, where data flows across borders in an instant. The problem is that while data is borderless, data protection and privacy laws are mostly national. We must meet this challenge.

I have already committed in my Strategy as the European Data Protection Supervisor for the next five years to invest in global partnerships with fellow experts, non-EU countries, authorities and international organisations to work towards a consensus on principles that can inform binding laws, the design of business operations and technologies and even the scope for interoperability of different data protection systems.

After listening the today's first keynote, I have the feeling that the bridge-building process has begun and that it is gaining strength. We are well aware of the differences between our systems of protecting the privacy of the individual.

But I propose for a change to start the conversation from our common values and from the things that unite us. Perhaps we will be surprised to find out that these differences are not so fundamental and that we can build starting with what we have in common.

Perhaps we can agree that the ultimate purpose of the systems of data protection and privacy, irrespective of their territorial origin, is to protect the freedom of the individual to control how his or her personal information is handled and by whom.

Talking about commonalities, we could perhaps point out that the draft US Consumer Privacy Bill of Rights Act talks about "personal data" and defines this concept, with some nuances, as data "linked or as a practical matter linkable (...) to a specific individual". This may sound familiar to those of us working with EU data protection law.

I had the opportunity to talk in the past year with colleagues from Japan and Brazil about their initiatives to adopt general data protection laws and I found common values and common themes that we all care about.

The Council of Europe is working hard on the modernisation of Convention 108, an important instrument that gained global reach once Uruguay joined it in 2013. Indeed, at present, Morocco, Senegal and Mauritius have expressed their intentions to become signatory states and they are in different stages of this process.

After revising the Privacy Guidelines last year, the OECD is currently focused on an initiative to analyse the role of data in promoting innovation within a multi-disciplinary project on "New Sources of Growth: the Knowledge-Based Capital". One of their aim is to provide policy guidance to mitigate the risks of Big Data and to ensure trust in the data-driven economy.

Therefore, I strongly believe that it is possible to have pillars of this bridge in different corners of the world.

Converging global responses are necessary due to the big challenges that are brought by the Big Data.

If I were to mention only some of the risks that big data pose to the protection of personal data, I would say:

- Challenges to user control, consent and self-determination of the individuals;
- Difficulty in allocating responsibility in the complex big data ecosystem;
- The lack of transparency;
- Re-purposing data, or the risk of using inaccurate data, taken out of context, for incompatible purposes;
- Potential for unfair discrimination stemming from biased conclusions based on correlations versus causation.

Big data challenges regulators and independent authorities to ensure that the basic principles of privacy and data protection are effectively applied in practice.

How can we reply to these challenges?

An important element of my Strategy for the next five years is promoting "big data protection".

The vast potential impact of Big Data and its associated technologies on individuals makes the ethical dimension of the response to these challenges unavoidable.

Accountability of the data controllers is essential in this respect. Big Data that deals with large volumes of personal information implies greater accountability towards the individuals whose data are being processed.

So what should we understand by "accountability"?

Accountability requires that controllers put in place internal mechanisms and control systems that ensure compliance and provide evidence - including internal policies and audit reports - to demonstrate compliance to external stakeholders, including supervisory authorities.

There are many elements that make up good and accountable practices. For instance, accountability underpins network and information security, including the current model of risk management for security.

Another key element is privacy and data protection by design. It aims at building privacy and data protection into the design specifications and architecture of information and communication systems and technologies.

Data Protection by Design is not limited to technical aspects; organisational measures are just as important. Data Protection Impact Assessments, auditing and certification may each contribute and form an integral part of an accountable internal control system.

These instruments should be required and encouraged as appropriate as they may play an important role in ensuring that big data is used responsibly.

Another tool necessary to ensure accountability is the introduction of a general data breach notification obligation. The new rules will create a strong incentive to allocate responsibility for the prevention of such breaches at the appropriate level of the organisation.

Finally, individuals must be able to understand how algorithms can create correlations and assumptions about them, and how their combined personal information can turn into intrusive predictions about their behaviour. Accountability means giving clear information to individuals about:

- Who is responsible for collecting and using the information,
- The purpose of doing so,
- What information is processed, whether it is knowingly volunteered by the individual, or whether it is observed and inferred without the individual's knowledge,
- How information is processed including the logic used by algorithms to determine assumptions and predictions about individuals,
- How long the information will be stored and with whom it will be shared.

Another type of response we can give is of a legislative nature. The European pillar of the bridge I was mentioning before is currently under "renovation".

It is important that the reformed data protection rules remain consistent with existing principles, including necessity, data minimisation, purpose limitation and transparency. These principles provide the base line we need to defend in order to protect our fundamental rights in a world of Big Data.

These are the same principles the demand that the State and its security and law enforcement arms access and use personal information proportionately, and with the maximum possible transparency without compromising their legitimate goals of protecting the public.

At the same time, these principles must be strengthened and applied more effectively. They must be applied in a more modern, flexible, creative and innovative way. The reformed data protection rules have the potential to fill with content the principle of accountability.

Most of all, they must be complemented by new principles such as accountability and privacy by design. The reform process plays an important role in this respect.

One of the main achievements rightfully expected from the General Data Protection Regulation is harmonisation. I believe harmonisation is key for businesses and individuals. The Regulation has to be truly European in the letter of the law and how it is applied through enforcement mechanisms.

But there are expectations that the Regulation will achieve more than this, including with regard to Big Data and its challenges for data protection. I would like to emphasise the potential value of the EU data protection reform in facing the Big Data challenges.

1) I support the application of the reformed legal framework to processing in its entirety, *both to use and collection of data*. A differentiation in this regard has never been made in EU data protection law and it has the potential to weaken the protection of fundamental rights.

2) There is no justification for blanket exceptions for processing of pseudonymous or anonymised data or for processing publicly available data. Currently, I am concerned with regard to some exceptions for processing publicly available data that seem to be taken into account in the legislative process of the proposed regulation and I hope that they do not remain in the final act.

3) The definition of personal data must remain intact. We have seen recent court decisions at Member State level that effectively applied this definition to scenarios similar to big data, by underlining that "data that 'individuates' the individual, in the sense that they are singled out and distinguished from all others" is personal data and is protected by the data protection law.

4) There should be no loopholes for processing of data on an excessive interpretation of legitimate interest grounds, and consent should continue to be required where appropriate. Nevertheless, it is true that accountable practices sometimes can go a long way to allow processing in the absence of consent.

5) It is important that when consent is required, it should be a genuine one. Mere ticking a box without understanding what we agree to, and without meaningful choice

whether we do so, must not be sufficient to signify our consent for complex big data application.

6) Transparency should be reinforced to ensure an end to secret profiling and should include disclosure of the logic of decision-making. Let us not forget that access to data and information on the details of the processing operation are a solid part in the content of the right to personal data protection as enshrined in Article 8 of the Charter of Fundamental Rights of the EU.

7) A powerful right to data portability may serve as a precondition to allow users more control over their data, and may also help contribute to more efficient markets for personal data, to the benefit of consumers and businesses alike.

Data portability is not only good for data protection, but also for competition and consumer protection: In particular, it can foster a more competitive market environment, by allowing customers more easily to switch providers.

Therefore, I strongly support the inclusion of a strong right to data portability in the proposed Regulation, as well as the inclusion of this right in relevant sectorial legislation, regulation or guidance.

The aspects I pointed out above indicate that there is real potential for the proposed Regulation to counter the risks that Big Data pose to the fundamental rights of the person. I hope that this potential will be entirely met in the adopted legislative act and I will exercise entirely the competences of the EDPS towards this result.

A third type of solutions to the Big Data challenges are of a technical nature.

I have already mentioned above that Privacy and Data Protection by design, as well as network and information security are a significant component of accountability of controllers in the Big Data world.

What we need to do is to promote technologies that enhance privacy and data protection. This is another action of my Strategy for the next five years. We need

- to enable privacy engineering by working with IT developers and designers;

- to collaborate with academia and researchers in the public and private sectors in order to contribute to innovative privacy friendly technologies;

- to focus on the importance of cyber-security and the collaboration between stakeholders so as to ensure that the cyber-security issues are dealt with as efficiently as possible;

- to highlight that promoting privacy friendly technologies triggers consumer trust, which can encourage business growth.

In this sense, perhaps it is important to advocate a change of perspective for business. In my view, data protection rules are not intended to choke creativity, but rather to provide a condition for success and competitiveness.

There are plenty of examples of start-ups who seek competitive advantage through their privacy policies. But the market for privacy enhancing technologies is weak, as attested by the low number of patents for PETs compared to those granted for data analytics.

Finally, solutions to Big Data challenges would lack efficiency in the absence of enforcement cooperation.

Collective risks require collective responsibility and collective response.

At the same time, the big risks involved by Big Data require a big response. For instance, a breach of EU competition law can cost the responsible body 10% of the annual revenue. This shows, on one hand, that the EU places a great deal of value to fair competitiveness. On the other hand it also shows that such important sanctions against unlawful behaviour of companies and service providers are possible. They should all the more so be possible when fundamental rights are at stake.

There are various fora for enforcement cooperation within the EU and internationally. We should work towards strengthening them.

At the International Conference last year in Mauritius the representatives of data protection authorities and privacy commissioners from all over the world agreed on the

Enforcement Cooperation Arrangement that should become open for members to adhere to after the International Conference in Amsterdam, this year.

The GPEN Alert is another initiative towards enforcement cooperation that can be helpful at least in identifying a contact authority in case of a cross-border complaint.

As far as the EDPS is concerned, I intend to promote a better and deeper interaction with APEC.

At the same time, I am an advocate of simplifying the rules where possible and of promoting tools like standard contractual clauses to enable lawful data flows.

Let me conclude by *just pointing out a few of the practical steps that the EDPS has taken recently and the ones that we committed in the near future.*

The EDPS has already begun to have an active role in the Big Data debate. We want to encourage a better informed conversation on what Big Data and the internet of things will mean for our digital rights. These are not merely European issues, but global concerns. And this is why the bridges I was mentioning in the beginning are so important.

Last year in June we organised a workshop in Brussels on competition, data protection and consumer protection attended by experts from the European Commission, national regulators, academics and NGOs, as well as the US Federal Trade Commission. It was a very useful learning exercise, which provided the basis for significant strategic actions we committed to for the next five years.

One of the initiatives I energetically support is establishing an external advisory group on the ethical dimension of data protection to explore the relationships between human rights, technology, markets and business models in the 21st century, analyse the impact of Big Data in depth, assess the resulting changes of our societies and help indicate the issues that should be subject to a political process.

Another tangible contribution to these discussions is the Internet Privacy Engineering Network – IPEN – which we established last year together with other data protection authorities and partners from industry, academia and civil society. It brings

together different disciplines and developers from different areas to work together on implementing practical privacy.

Ladies and gentlemen, we want to encourage a better informed conversation on Big Data and the internet of things and what it means for our digital rights. These are not merely European issues, but global concerns.

And this is why the global bridges I was mentioning in the beginning are so important.

I want to thank you all for your attention and to invite you to take part in this conversation.