Keynote speech to the IAPP Europe Data Protection Congress 2016

Brussels, 9 November 2016

Giovanni Buttarelli

Ladies and Gentlemen,

It's a pleasure and a privilege to be here, after an unexpected two year break.

The world looks a lot different than it did in November 2014. In ways, which none of us would have predicted.

Few of us would have predicted such a deadly resurgence of terrorism in the heart of Europe that would have disrupted everyday life in Belgium and France. Including of course the cancellation of last year's IAPP Congress.

Few of us would have predicted of the UK voting to leave the European Union.

None of us would have predicted such a colourful and angry US Presidential Election.

We might have predicted that, at long last, the EU would reach agreement on the new data protection framework.

My message to you today is simple:

Get ready for the GDPR, but continue to expect the unexpected.

It is already six months since the GDPR and the Police Directive became EU law. There are now 18 months to go before they become fully applicable on 25 May 2018.

That is 533 days to be fully compliant with the 99 Articles of the Regulation.

For the Directive applying to competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, Member States have a little less time to fully transpose in national law - the deadline is the 6 May 2018.

The ball has been dispatched by the legislators and now it's firmly in the court of the regulators like us on this panel.

Our big challenge is to help controllers ensure that the abstract letter of the law becomes a concrete reality on the ground.

99 articles in 533 days.

Make no mistake: the GDPR is here to stay for a long, long time.

We need to focus on what is desirable as well as necessary.

But the perfect should not be the enemy of the good.

My institution was never a party to the negotiations on the legislation, but we were fully engaged in fulfilling our advisory role - like all independent DPAs - to the co-legislator.

We were able to leverage our years of experience as a supervisor and policy adviser to identify ways to improve the text, to focus on safeguards for individuals not bureaucratic procedures.

You might recall that we produced an app, free to download, so that anyone can compare more easily the old directive and the new regulation.

One of our big priorities was to make data protection simple.

I am pleased that we were successful to some extent.

21 provisions for implementing or delegated acts by the European Commission were replaced to allow independent DPAs to consider targeted and relevant guidance for controllers and processors.

In the Article 29 Working Party, we have a unique opportunity now to develop a new gold standard for forward looking and practical guidelines.

The outcome needs to be user friendly and draw from best practice across the EU and outside the EU.

The process needs to consult and to be accessible and transparent with stakeholders. That is now an obligation under GDPR Article 70.4.

Our independence as DPAs is precious and its value, in this volatile age of big data and mass surveillance, cannot be overstated.

We have now extensive case law setting out the requirement for functional and visible independence from the executive.

But independence is not isolation.

No DPA sits in an ivory tower. Nor should they.

We need to be conversant with technology in order to better assess its impact on personal data processing and fundamental rights.

But we also need to be conversant with technology to enable more efficient and inclusive discussions among ourselves as a community of DPAs and with stakeholders in this room and elsewhere.

We need to be open and establish a new normal for discussion and debate with controllers, on the basis of accountability.

Accountability contains the notion that failure to comply, causing harm to individuals with irresponsible data processing, must be addressed.

The GDPR gives us the ability to apply proportionate and dissuasive sanctions.

The sanctions must be scalable, just like the obligations throughout the GDPR, in accordance with the riskiness of processing operations.

We have discussed for example how to 'set the dial' between core activities and large scale processing, and how this should influence whether a DPO should be appointed. And how to assist SMEs who may not have the resources to employ a dedicated DPO.

We have been discussing the new right to data portability and the sectors, in which it would be relevant, its relationship with consumer, competition, and IP law.

We have discussed how to roll out data protection impact assessment, the types of risky processing operations, which would require one.

And we have discussed the role of certification - a really important innovation for accountable data controllers and for rebuilding trust among individuals the era of hyperconnnectivity. We need to clarify the roles and responsibilities of the various players in this new arena - including DPAs, the Commission and accredited certifying bodies.

So the system needs to be affordable.

More than anything, the system must be credible.

People are entitled to expect an acceptable standard of protection and respect from companies and governments handling their personal data, as they would expect from someone handling your private property, or for handling machines or using medicine.

This is an uncertain period for society and the economy.

Nassim Taleb in his 2007 book Black Swan writes eloquently about how, in predicting the future, we tend to ignore isolated events and negative results.

We ignore how people are driven by infinity of instincts. And most of our history is silent, and undocumented.

The EDPS Ethics Advisory Group is working intensively on a set of principles, which can help policy makers and DPAs to navigate existential waters: on what it means to be human in an age of virtual and enhanced reality and artificial intelligence.

New ethical questions are emerging all around us.

Everyone is talking about the Netflix series Black Mirror and its kaleidoscope of technological dystopias.

In one episode, your online reputation literally determines the ability of people to participate in society and the economy at any level.

It may seem ridiculous. But we know the recent story of a UK insurance company wanting to make use of social media data in determining what policies to offer to clients.

And we know about the social credit initiative in China.

We have to build on the ethical and legal framework, which is in place, to shape technology and revenue models. It should not be other way around.

Ladies and Gentlemen,

We will probably come to Brexit during discussion.

But one country leaving the EU doesn't change globalisation.

There is a movement against international flows and common standards, a tendency to protectionism - which we have seen in the debates during the US Elections as well as the political debates in the EU.

But we must meet these challenges on the basis that data flows, subject to the correct rules, are meant to benefit society and individuals.

Respect for different legal cultures implies reciprocity.

Adequacy is not imposition and data protection is not a trade barrier.

These are opportunities to build bridges and learn from one another.

Thank you.