8th Annual Data Protection and Privacy Conference

Brussels, 30 November 2017

Keynote speech

Giovanni Buttarelli

Thank you to Paul and Forum Europe for the invitation to this 8th edition of the European Data Protection and Privacy Conference.

It has taken eight editions - but one more will be required before the GDPR will have become fully applicable.

This is the last big data protection jamboree of 2017.

And EU regulators met yesterday for the last time this year in plenary of the Article 29 Working Party, and also for the last time under the current chair of the Working Party.

If anyone of you doubts the work rate of European DPAs, you should take a look at the gargantuan bundle of papers which each commissioner had to carry into the meeting.

Our discussions ranged from the Privacy Shield to consent and transparency through to the procedures governing the EDPB from May.

So the end of the year is always good moment to take stock.

The landscape continues to evolve rapidly.

But the overall trend is towards redressing the imbalance between individual and powerful state and commercial actors.

This is an imbalance which has increased alongside the digitisation of society and economy in the last 20 years, alongside the obvious benefits.

So the end of last year the European Court of Justice in the Tele2 Sverige case reaffirmed that generalised and indiscriminate surveillance is not permissible under EU law.

2017 began with, in January, the European Commission's proposals on ePrivacy and reform of the general data protection rules for EU institutions and bodies - the 'other GDPR' for EU officialdom.

These are new approaches to regulating the flow of data and interference with private communications.

But this is not just about the stick of enforcement and sanctions and fines.

These approaches are, more importantly, about the carrot of incentivisation.

That is my message to you at the beginning of today's discussions:

We need to incentivise privacy friendly engineering and better-informed individuals.

So let's look beyond the GDPR.

I would like to set the scene for our discussions. Then I will talk about how we regulators are preparing for our new responsibilities.

Then I will address why we think the ePrivacy regulation is so necessary before looking even further into the future of regulation.

The digital economy continues to evolve rapidly.

But it has become increasingly concentrated, with the same dominant players in a position of dominance for now over a decade.

Their power in terms of market capitalisation is far greater than that of the big oil companies whom they have replace in the list of most valuable companies.

A similar trend has been observed with the concentration of AI expertise.

The centralisation of these capabilities has been lamented by the pioneers of both AI and the internet itself, such as Tim Berners Lee.

AI raises fundamental questions of accountability for outcomes, as well as accountability for collection and use of massive quantities of personal data.

And without massive quantities of data, AI would not be possible.

For over a decade, the Silicon Valley nostrum 'move fast and break things' has been enough to minimise regulation... and also to minimise accountability for the side effects of innovation and business success.

This is where the GDPR and other reforms step in.

You could say that the spirit of the GDPR is encapsulated in Recital 4 - The processing of personal data should be designed to serve mankind.

People are no longer willing to tolerate so many broken things.

So we are starting to agree standards which need to apply in the digital space, just as digital natives, millennials, begin to enter the world of work and reach voting age.

There is now a market for not just personal information but also attention.

There is a recognition that the current dominant business model is not sustainable.

Let me offer an anecdote.

In Leuven this month there was a meeting of the Internet Privacy Engineering Network, a group of engineers and developers who want to put privacy by design into practice.

We heard a presentation on a study into how intimate data on our mobile phones are exchanged over 5000 times over the course of two weeks, including with mysterious third parties.

We are either unaware of this, or we have conceded access to all the private information on our device to the apps in question.

People are starting to revolt against this.

The ad blocker war can be seen as just a proxy for the real confrontation:

A confrontation between a more technologically aware generation (my children's generation!) who do not want information about them to be used in ways that they cannot even understand, let alone or control.

Yesterday I had my first exchange of views with the European Commissioner for Digital Economy and Society, Mariya Gabriel.

One of her priorities is to investigate the phenomenon of 'fake news'.

Like ad blockers, you could say that fake news controversy is also a proxy for the real problem: data is being collected without peoples knowledge and people are being put in categories which they cannot contest.

This is a new and disturbing front for defenders of the right to data protection.

The controversy over voter micro targeting has highlighted the importance for democracy of data protection and respect for communications confidentiality.

This is a strategic issue, in my mind, for all DPAs, and I intend to publish a preliminary opinion on the subject early next year.

As I said earlier this month at the IAPP Congress, the 25 May 2018 is not going to be the end of the world as we know it. It is more like the beginning of the beginning.

The GDPR is an essential, major piece of the jigsaw. But it is only one piece.

There is also the way it is enforced, coherently with other regulators.

Article 60 states that 'the lead supervisory authority shall cooperate with the other supervisory authorities concerned in accordance with this Article in an endeavour to reach consensus.'

There is great scope for convergence – a long way to go - like with other areas like antitrust and financial services regulation.

Look for example at budgets for individual authorities in proportion to the number of people they are meant to protect – that in relation to population.

There are massive disparities – from 50 EUR per 1000 population in one Member State, to almost 8 000 EUR in another!

With the EDPB, EDPS is going to have a big role.

The EDPB will be an entity in its own right - potentially very powerful.

There will be inevitable tension between the constitutionally enshrined independence of action of every DPA and the legal obligation for them to cooperate.

That is what makes Article 65 of the GDPR - which provides for dispute resolution procedure where a lead authority has rejected the objections of another DPA - so extraordinary.

It would require, once invoked, a binding decision of the Board, with the Chair having the casting vote if the votes are split, requiring an independent authority to implement a decision which it may disagree with.

I think this is a legal fiction.

It is a means to push DPAs towards resolution under the general requirement to act in the interests of consensus.

We will do all we can to ensure that the EDPB is a success, as a loyal member of the body, and as the provider of the secretariat.

We need a spirit of unity among national DPAs in the EDPB, according to the GDPR the principles of collegiality and accountability - and efficiency.

So expect a lot more work via video conferencing rather than costly meetings in person.

DPAs will not have the luxury of discussing the limits of their own jurisdictions and competence; instead they will have to devise together a new approach.

It is time to keep the best from national experience as part of a new common approach

Companies and other stakeholders represented in this audience have the right to expect that, with the GDPR, there will be a single email address and phone number for EU data protection

But the EDPB, like the best Christmas presents, is not something to be appreciated only at Christmas.

On the other hand, the EDPB like all legal instruments, cannot live forever.

The GDPR will applies wherever a service is offered - and this is completely proper, because data flows and regulation are going global.

I am confident that the EDPB will be a success – to provide legal certainty, reliability and most of all as the champion for individual data subjects.

But the board needs to be as least as great as the sum of its parts.

There are may be altogether around 2500 people working for DPAs in the EU.

This is a fraction of even the number of people employed to lobby the EU institutions in Brussels.

So we have to work together and focus on the biggest problems, and do everything to promote a culture of accountability among controllers.

Advice to controllers

And on the subject of the GDPR, the best advice to controllers is to try not to think about fines. There will be fines - eventually.

But the focus now needs to be on trust and confidence that controllers are taking their responsibilities seriously.

What do I mean by taking responsibilities seriously?

Controllers first of all need to be clear about what data is being processed and who is responsible for it

Second, there needs to be a genuine evaluation of risk - forget formalistic but empty and meaningless DPIAs.

And what about trade deals and adequacy and transfers of data out of the EU - the subject of the first panel discussion today today.

This week the WP29 discussed its response to the first review of the Privacy Shield agreement.

No one is questioning the principles.

Even the implementation and enforcement are less of a concern, though there are some complications to assess what is really happening because of the self-regulatory model.

And even the arcane question of independence of supervisory bodies in USA may not be the biggest problem.

We keep talking about independent ombudsman, but we may be need a different approach in the future which take account of how the US Constitution works.

The real problem, from a fundamental rights point of view, is mass surveillance.

So we still need a longer term solution - that's why GDPR provides for a review of adequacy decisions.

The attention economy and why ePrivacy matters

Now I want to turn to the reason why ePrivacy is so vital to this new generation of rules.

It is already an old and discredited cliché to say that data is the new oil.

But the analogy could be stretched in different ways.

For example if you compare legal standards to an oil tanker which takes a long, long time to change direction.

Your agenda for today reflects the way questions of privacy and handling data have spread out from the esoteric world of internal bureaucracy to almost every significant strand of global dialogue.

From trade to international banking, from humanitarian relief to predictive policing.

The standards under discussion today need to set a framework for all of these digitally enabled activities.

It is ironic that Europe is a leader in updated values and rules for the digital era while it continues to lag behind in terms of innovation and success.

The GDPR, ePrivacy, the growing body of case law represent a business opportunity for another looking to tap into a market of half a billion people, most of expect to get more control over their data.

But in fact there are a number of ways in which the EU like other countries around the world are responding to society's extraordinary 'digital turn'.

The really big strategic challenge is for DPAs and controllers to think through the ethical implication of how technology is evolving.

Make no mistake, ethics is not a soft law alternative to compliance.

Ethics is the underpinning for genuine compliance, for avoiding box-ticking approaches which undermine trust in digital services.

In February, the European Parliament adopted a resolution on AI which touched on the question of whether robots should have rights and obligations.

The irony, is rather exquisite, when you think about it: the dominant business model for online services treats human beings like robots.

As a result, our brains are being farmed for content and data.

Connected things and software are designed in order to addict people – especially children – look at the controversy in China among parents worried about the effects of a mobile game.

This is a game which generates half the income of one of the world's biggest internet gaming companies.

The attention of a human being is limited and bound up with his or her intimate space- in other words, it is privacy.

There are issues to be resolved in trilogue, like the relationship with GDPR and important technical questions.

But ePrivacy, if it succeeds, will change the incentives in the market.

It will shine a light on covert tracking and scanning of private communications

Finally, as requested, let's look further into the future.

My vision is for there to be, by the mid-2020s, a truly European board which is visible, credible and accessible.

I know that there are calls for a single digital regulator, to ensure companies fulfil their obligations across a range of sectors, not only data protection and privacy, but also consumer protection and various rules on product safety and antitrust (in the case of dominant players)

The German competition authority is investigating whether Facebook abuse its dominant position through imposing unfair data use policies.

So we need to find a way of harnessing the existing effective tools and ensuring they are used coherently with tools for data protection and electronic privacy.

The world is racing.

The EU has just taken a decade to reform its data protection rules.

We know that in a decade smart devices have become, in effect, an extension of our bodies.

Smart phones today are more powerful than the most powerful supercomputers twenty years ago.

So we cannot be left behind.

We have to keep the law under review, evaluate whether it's having the desired effects.

Is the GDPR ensuring that handling personal information is serving people, not the other way around? That is the question at the top of our minds as independent DPAs.

We also need to show guts, as well as skills and expertise, keeping in the mind the big picture that data processing is essential to economy and society.

The EU has had a rough time in recent years.

But we have to stay optimistic.

Brussels is not the devil. The GDPR and EDPB is our business card for showing the world how we can regulate big data and AI.

We need to increase proximity to citizens.

I am looking ahead already to the next reform – we will begin discussions in next decade.

Why should we not aspire to building a body which draws inspiration, for example, from the Federal Trade Commission in the United States. One possible way would be a single body with an explicit obligation to act in the interest of all data subjects in the EU, a bit like the oath which Commissioners must take when they take office.

So thank you for your attention. I look forward to answering any comments or questions you might have.