Privacy in an age of hyperconnectivity

Keynote speech to the Privacy and Security Conference 2016

Rust am Neusiedler See, 7 November 2016

Giovanni Buttarelli

Ladies and Gentlemen,

Thank you to Rainer Knyrim and Martin Szelgrad for their invitation to this conference on Privacy and Security.

It is a great pleasure to join you in such a beautiful part of Austria.

It was just over a year ago that, as a result of the persistence of a certain Austrian law student, data protection became headline news across the world.

The *Schrems* judgment from the European Court of Justice of October 2015 affirmed a number of core data protection principles, including the independence of data protection authorities and the requirement that personal data should only be transferred outside the EU where the safeguards are 'essentially equivalent' to those which apply under EU law.

It changed the landscape, and provided fresh impetus to policy makers- in the EU and United States in particular - to build bridges across a diverse world.

Data protection and privacy have become urgent public policy priorities.

The reason is that it is no longer the case that a simply few details about our private and professional lives are being recorded and stored in metal filing cabinets.

Our lives are being documented constantly, usually without our knowing, and stored indefinitely as a result of big data technology and the proliferation of sensors as we move towards the internet of things.

And these are not just raw data. Information has always been power, but big data is valuable because of the inferences which can be made, increasingly by artificial intelligence and machines that learn.

AI and Robotics and data are, as EDPS wrote in his recent discussion paper for the International Data Protection and Privacy Commissioner Conference in Marrakech last month, a two way street. Personal data feeds AI, and AI produces more inferred data.

We are right to be healthily sceptical of Big Data evangelists who preach big data utopia.

But neither should we fear a Big Data dystopia.

Big Data may offer tremendous benefits to individuals and society, in the areas of health, transport and environmental protection.

Data protection, and real choice and freedom to communicate privately online – these are essential to ensuring that the big data dividend is spread to everyone, and not only to those who can afford it.

So I want to talk to you for a few minutes about what we call the Big Data Protection Ecosystem.

And I would like to talk about how the new rules in the EU in the General Data Protection Regulation fit into that Ecosystem.

Data protection in the EU has always been about facilitating the functioning of the internal market, through rules which protect the individual.

This is a fact that is too often overlooked.

Protecting the rights and interests of individuals is not a trade barrier. It's a facilitator of trade, because it sets out the rules and builds trust, like other areas of law like on anti-money laundering. The solution is not to abandon necessary rules but to cooperate better, and make them more predictable and efficient in how they are enforced.

But personal data protection is no longer simply a matter of law-making and legal compliance.

Modern and sustainable laws, effectively enforced, are one part of the Big Data Protection Ecosystem.

That is why independent DPAs - like your local authority in Austria, led by Andrea Jelinek, and my own the EDPS - invest so much effort into cooperation and information sharing.

In the digital era, there are multiple agencies responsible for ensuring the interests of the consumer are safeguarded.

That is why we have proposed for the first time a cross-jurisdiction network for consumer, competition and data protection authorities to talk to each other about their common concerns - an initiative called the Digital Clearing House.

We hope that it will be a useful resource and help ensure more coherent and efficient enforcement.

It took four years for the EU to agree the General Data Protection Regulation. It is in force now but it will fully applicable as from 25 May 2018.

That may seem a long way off, but it is not.

Think about it – it is six months since the GDPR was adopted: already one quarter of the time to be fully compliant has elapsed.

That is why this conference is so important.

Preparation for May 2018 is a matter of urgency not only for companies but also for data protection authorities who will compose the one stop shop and the consistency mechanism.

A second component of the Big Data Protection Ecosystem is accountable controllers.

The core principle of the reform is ‘accountability’ principle runs through the core of the GDPR.

I know that the German translation used in the GDPR '*Verantwortung'* – is an imperfect translation.

As I wrote in my blog earlier this year, the notion of accountability is very old. It comes from the Latin for 'to reckon', and so it's actually closer to the German word for bill or check - *Rechnung*.

Processing personal information is not prohibited, but it comes at a cost. It affects the rights and interests of the individual concerned by the data. So it is right for anyone who profits from the data to *give account* for what they have done and why.

Not only commercial organisations of course – the need for such 'reckoning' stretches across all sectors that handle personal information, including government, private, academia, commercial, and not-for-profit.

And so Article 24 of the GDPR requires organisations to implement 'appropriate technical and organisational measures' to be able to 'demonstrate' their compliance with the Regulation, which shall also include 'the implementation of appropriate data protection policies'.

It means internal and publicly-facing policies, records and notices, but also technical measures, and fundamental personnel and strategic changes to their processing operations.

It means being able to demonstrate compliance with the data protection rules – a shift from a merely bureaucratic compliance exercise.

It signals a genuine culture change.

My institution and all independent DPAs need to be fully accountable also.

The Article 29 Working Party plans to meet five times in full plenary next year, in addition to meetings of the various subgroups, at rate of almost one per week.

The GDPR goes into great detail on many things – in some cases perhaps too much detail! But one area which is described in detail is the requirement for cooperation between DPAs. The old Directive 95/46 had one sub-clause with a general obligation to cooperate. The GDPR has six substantive articles covering information sharing, joint operations and mutual assistance.

We will be working intensely to ensure that the EDPB is an accessible, transparent and accountable body. We will aim to provide as much legal certainty as possible for controllers, including through the publication of relevant and user friendly guidance.

The Working Party has undertaken, in its current work programme, to issue guidance for controllers and processors on the right to data portability, the notion of high risk and DPIAs, on certification and DPOs.

My priority as data protection authority for the European Union institutions and bodies is to promote accountability so that we lead by example in the new digital reality.

That is why, today, I have published two sets of data protection guidelines on how EU bodies offer web-based services and mobile apps.

That is why I have been meeting at the highest level EU leaders, including the presidents of the European Central Bank and the CJEU as well as the big institutions of the European Commission, Council and Parliament.

The third component of the Big Data Protection Ecosystem is privacy conscious engineering.

The EDPS coordinates the Internet Privacy Engineering Network, set up in 2014, which brings together different disciplines and developers from different areas to work together on implementing practical privacy.

I encourage you all to follow this initiative – the information is on our website – because it is very relevant for the discussions which you will have today and tomorrow on cyber security. We need to work together at on technical and policy solutions. Security is key to the sustainability of our digitally supported economy and society in preventing and responding to cyber disruptions and attacks which are becoming ever more frequent and unpredictable.

Cybersecurity is needed not only for our own infrastructure but also for the global network. We need a high common level of network and information security to ensure effective security across the board.

Of course the GDPR is only the biggest piece of the whole data protection puzzle.

Early next year the EU will begin negotiations on the reform of the ePrivacy Directive. This is uniquely valuable because it is the only secondary law instrument that protects the confidentiality of communications; it is the modern day equivalent of traditional postal statutes guaranteeing the secrecy of correspondence.

The Digital Market and information society need confidentiality of communications to be able to function effectively. We have argued that it is crucial to have specific rules for all communications services – a level playing field.

We have called for all arms of the EU to work together to promote conditions for more privacy and freedom online – what we have called a Cyber Commons - where you can interact online without fear of being tracked and unfairly categorised.

We will also see next year the reform of Regulation 45/2001, which governs how EU bodies process personal information.

This will need to cling as closely as possible to the GDPR, no special treatment for EU public bodies where not justified.

It will also need to uphold the principles of the independence of data protection authorities.

We know from three judgments by the CJEU, in addition to the more recent *Schrems*, concerning the situation in Germany, Austria and Hungary, that the independence of DPAs from the executive must be functional and demonstrable.

Several fundamental rights are at stake in the age of hyperconnectivity, and not only data protection. Privacy and freedom of expression - two sides of the same coin – are threatened when most people have little meaningful choice about where they consume content online, and very limited choice to opt for web based services which do not track your behaviour. The right to non-discrimination is threatened when the inferences made from the masses of personal data collected result in profiles and decisions which are opaque and cannot be challenged.

That was our message in our recent Opinion on Coherent Enforcement, and the reason we are calling for a Digital Clearing House bringing together all agencies with the goal of upholding the interests of the individual.

Vienna is of course the home of the Fundamental Rights Agency. We work closely with the agency and the new director Michael O'Flaherty and I recently agreed to step up this cooperation, including next year with the agreement of a Memorandum of Understanding between our two organisations.

Finally, the fourth component of the Big Data Protection Ecosystem is empowered individuals. We do not advocate paternalistic solutions, treating individuals as passive vulnerable objects who need the protection of state authorities.

We want to encourage solutions which give people control of their own lives online.

Last month I issued an Opinion on Personal Data Management Systems and how they could, with a bit more support from the EU, enable people to know and control what happens to their personal information.

Ladies and Gentlemen,

I look forward to discussing with you the challenges of implementation of the new rules. I would encourage you to be as open and honest about your concerns and questions with the Austrian DPA, which has brilliant experts on how the law works.

There are only eighteen months between now and May 2018.

There is much to do but we are laying the groundwork for a new generation, a generation for whom hyperconnectivity is the only lived reality they have known.

So thank you once again for your attention.