Data Protection Day 2020: Facing New Challenges

Croatian Presidency of the EU Council Conference

16 January 2020

Wojciech Wiewiórowski

Zagreb, Croatia

Thank you, Maja, for the kind introduction.

Deputy Prime Minister Božinović, Minister Bošnjaković, Minister Malenica, ladies, gentlemen and distinguished guests,

It is a great privilege to address this event today.

It is a new year, a new decade, so it is appropriate that the newest Member State of the EU assumes the presidency of the Council for the first time.

And as European Data Protection Supervisor, I am greatly encouraged that the Croatian Presidency have chosen to host such a high-profile event dedicated to data protection.

Croatia adopted its first EU-style data protection law in 2003, and like my country Poland, the law was grounded in the right to privacy in the national constitution.

I see that your constitution also includes a specific right to 'the safety and security of personal data'.

You may not be aware of this, but data protection in Europe celebrates this year its Golden Anniversary.

It is now 50 years since the first European data protection law was passed, in the German Federal State of Hesse in 1970.

The state's lawmakers were reacting to the creation, in 1969, of an integrated data processing system for government data.

Excitement about the benefits of automation gave way to concerns about loss of privacy and too much power for the state.

Members of the Hessian assembly looked at reports from US Congress, prepared a bill and adopted a law on 30 September 1970.

It was the world's first data protection act, composed of 44 articles.

The Hesse law focused on public sector data processing, requiring it to be authorised by law or consent, with the right to information and block, the creation of a Data Protection Commissioner's office.

The now familiar triad of controller, supervisor and data subject was already sketched out in the Hessian law, though the terminology was still very fluid.

After 50 years - and 10 years since the GDPR was first proposed - some people may think that the appetite for more data protection law in the EU has been exhausted.

But at the start of this new decade, we can detect a shift in the tectonic plates.

Digitisation has taken over our lives in the space of twenty years.

Much of this exponential growth in connectivity and data processing was driven by private industry – especially companies located on the West Coast of the US.

Business models emerged which responded to a fanatical belief among investors that data was the new oil.

So services should be provided below cost, or even for 'free', in exchange for collecting data about people.

These data would be stored on proprietary clouds and monetised – typically through online advertising.

The tectonic plates are now shifting in a number of ways.

Firstly, Europe has always struggled to compete for market share with the companies which grew so quickly in US and more recently in China.

In particular, Europe doesn't seem to be in control of its own data. As European Commissioner for the Internal Market, Thierry Breton, said last week,

"Europeans should be owners of their data and those data should be processed in Europe, according to our rules and values. We cannot continue to live in a world where 5 or 6 big actors hold 80% of the data on the planet while not accepting responsibility for how the data are used."

Indeed, data localisation laws are spreading around the world. India seems set to join Russia and China in requiring at least 'sensitive data' to be stored within the national borders.

Secondly, people are starting to object to the constant tracking and targeting which the business models have relied on.

This week, Google announced its intention to end third party cookies on its Chrome browser.

And the UK data protection authority has said, in effect, that the online advertising ecosystem involves systematic violations of the GDPR.

The European Court of Justice is gradually clarifying what it means to give consent, freely and validly, to data processing - and exposing a number of day-to-day commercial practices as unlawful.

Thirdly, there is a generational shift taking place. Digital natives, post-millennials, Generation Z – or whatever you want to call them – are starting to graduate from school and enter the world of work, politics and activism.

They never experienced life without being connected to the internet.

They want to be in control of their digital lives, and they are starting to see governments and big companies – rather than parents and teachers - as obstacles to this control.

Again here, the EU Court of Justice is developing a body of case law which delimits the ability of the state to interfere with the rights of its citizens.

The Advocate General, in his (non-binding) opinions on three data retention cases this week, reiterated the incompatibility with EU law of blanket data retention of all communications data without demonstrably good reason.

This is a platform of jurisprudence for re-engineering digital society according to our fundamental rights and freedoms. We only need to rise to the challenge.

You can find many articles predicting tech trends for the 2020s.

They talk about cybersecurity vulnerabilities, computing on 'the Edge', quantum computing, augmented and virtual reality. They talk also, of course, of the deployment of artificial intelligence systems, and this will be the subject of this afternoon's panel.

But these online 'fortune tellers' also predict that the 2020s will be 'the privacy decade'.

Around the globe, more and more countries have data protection laws, usually modelled on European laws.

There are still gaps - notably in India and the United States - where there is no general data protection law, but we will see these gaps filled in the next few years.

Will Europe continue to be model regulator?

I hope so. But it is not certain or inevitable.

Data protection is fashionable now. But it is being used to advance state interests and corporate secrecy, perhaps more than it is used to protect individuals. So momentum must be maintained.

The Croatian Presidency of the Council has this month announced its priorities.

The priorities are to develop, to connect, to protect and influence.

It recognises the potential for digital policies to address the environmental emergency. That means technological solutions, of course.

But it also means doing *more* with *less* data – as even big tech companies are starting to admit. This is not only because of 'techlash', but also because processing terabytes of data consumes enormous and growing amounts of electricity.

The Presidency's strategy recognises the need for secure connectivity: as Internet of Things devices proliferate, so do the opportunities for malicious and hostile actors to exploit vulnerabilities.

It recognises the need for digitisation to enhance, not damage, freedom and democracy

Proposals will come from the European Commission soon in each of these areas: for example, the 'data strategy', the Artificial Intelligence White Paper, the European Democracy Action Plan, and the Digital Services Act that will address platform liability.

The Presidency will also prioritise unblocking progress towards reformed rules on confidentiality of electronic communications, ePrivacy.

Data protection is either highly relevant or at the core of these initiatives.

In the coming weeks I will publish a strategy for my new mandate as EDPS.

At the heart of our activities will be integrity.

If we are to be a credible, model regulator, the EU, and especially its DPAs, have to be beyond reproach in how we ourselves process personal information.

That is why we have been enforcing the rules in relation to EU bodies' contracts with Microsoft.

That is why I had to prohibit the European Asylum Office's scraping of social media data concerning refugees, which had no valid legal basis.

And that is why I had to reprimand the European Parliament for violations connected to its collection of personal data from over 329 000 people interested in the European election campaign activities, and allowing the data to be processed by the US company NationBuilder.

2020 will be a pivotal year for the EDPB, as the first major cross border cases reach their conclusions.

So, alongside Anto and his excellent team, I am doing all that I can to ensure the European Data Protection Board is credible and effective.

Over the next five to ten years, I want data protection to become not just a *barrier to irresponsible and harmful practices* – like trivial and unethical deployment of automated facial recognition technology.

I want data protection to be an *enabler of good practices*, which empower individuals and serve genuine public interests.

ePrivacy – which is about securing space in our digital lives which is free from monitoring - is just the start.

We need to re-imagine the sort of open, dynamic, respectful digital environment we want for our children and grandchildren.

Data protection authorities should be contributing to that not only through smart enforcement but also through engagement with big political questions and technological developments.

When the Commission refers to digital sovereignty, I hope that means what Commissioner Breton said: Europe in control of its data and using it according to its freedom and values.

As we celebrate our Golden Anniversary, that is something that the data protection community certainly can, and should, support.

Thank you.