21 February 2018

Commonwealth Data Forum

Giovanni Buttarelli

Thank you, Michael, for your kind introduction.

Thank you also to the Commonwealth Telecommunications Organisation and the Government of Gibraltar for their kind invitation to be part of this important event.

I am very sorry not to be able to be with you in person

As I am sure you will appreciate, there is a very heavy data protection schedule here in Brussels these days.

Ladies and gentlemen,

The "digital turn" in our society and economy is barely two decades old.

But the transformation has been deep and broad.

Data protection used to be about keeping filing cabinets secure from malign interference or unintentional negligence.

Most processing of information about people was, to use the term in EU law, for 'purely personal or household' purposes.

Data protection rules were not - and will continue not to be - concerned with such activities.

Instead, the rules were meant to improve the balance in the relationship between ordinary people and the powerful companies and public bodies with access to large quantities of information about them.

Europe, whether the EU or the Council of Europe, has always followed a balanced approach to the collection and use of personal information.

We want to encourage data flows because they are essential not only to the functioning of internal market, but also to society as a whole.

But we want to make sure that someone takes responsibility for these data flows.

We want to make sure that if you profit from using someone else's personal information then you need to show proper respect to them.

That is the theory at least.

The reality is that the rapid increase in computer processing power, and rapid decrease in the cost of data storage, has made it technologically possible to collect amazing volumes and variety of data, and to keep it indefinitely.

In the absence of legal or ethical constraints, the market will exploit whatever opportunities are offered by this technology.

So it is no coincidence that the engines of phenomenal digital growth are located in areas of the world where limitations on what you can do with data about people have been minimal or non-existent.

I refer of course to Silicon Valley, California.

But there are other Silicon Valleys - notably the Haidian District of Beijing for example.

According to the latest trends, China's tech industry will be equal in size and profitability to America's in 10-15 years.

China will have its own standards and values to promote.

This time framework coincidentally matches the timeframe between the GDPR and its eventual revision, if the 15 years between Directive 95/46 and the Commissioner proposal for the Regulation is a guide.

In the meantime, we already have a very problematic dominant business model for web-based services and connected things.

That model involves tracking people's movements, behaviour, even thoughts. Children especially.

Very often without them knowing about it, and often without them being able to object.

We are told that, by 2020, 1.7 megabytes of data will be created every second, for every person on earth.

This is the equivalent of a digital file of a short pop song - so a lot of pop music.

Is this personal or non-personal data? Who knows?

Even 'anonymised' and aggregated data can be technically used to identify individuals - so distinction between non personal and personal is likely to be obsolete.

So we need a sustainable digital agenda.

This year is probably the most important year so far in terms of legal response.

On 25 May the GDPR becomes fully applicable.

It will clarify the scope of the EU's data protection rules.

It will update rights and obligations for the big data era.

It imposes a new obligation to pursue privacy by design.

It will create a new model for inter-DPA collegiality and range of tools for enforcing the rules.

Most important of all, it will introduce the principle of accountability.

Accountability is the notion that controllers are responsible for complying and being able to show that they comply, but without having to notify every single minor data activity to the regulator.

The media like to focus on sanctions, and it is true that the GDPR provides for some serious penalties in the event of a serious violation.

On the other hand, sanctions can only be applied if a number of criteria are satisfied.

In any case, what is more important is the message we are sending to the world, that personal data is about the dignity of the human being, and the trust of the consumer.

Digital growth can only continue sustainably if these values are respected.

Already, entrepreneurs are starting to respond by developing products which minimise the amount of personal information processed, and which maximise the control the individual has over what happens to that data.

There is a vibrant debate now about how to make big data work for all of us, not just the privileged few.

We are exploring how antitrust, consumer law and data protection law can work together to stop digital monopolies from damaging freedom of choice and expression.

This, for me, is essential.

A million Euro fine here and there is not going to change the digital world.

We need a regulatory approach which empowers the consumer in the digital space.

Companies around the world who offer goods and services to people in the EU, or who monitor people in the EU, are subject to the GDPR.

There is already a lot of convergence of data privacy laws around the world. 121 countries, at the latest estimate, with laws largely modelled on those developed in Europe.

Even China has recently adopted standards which, in some ways at least (eg on companies use of customer data), may be judged stricter than the GDPR.

Of course simplest solution for companies is for as many countries as possible to be deemed by the European Commission to have an 'adequate' level of data protection.

Simple, also perhaps simplistic.

The assessment of adequacy is a complicated process. Only 11 states have achieved it, excluding the unusual Privacy Shield agreement with the United States.

That amounts to 2% of the world's population.

So the smart approach, I would say, is for companies to take a proactive approach to accountable data processing:

to know what they need data for,

to perform due diligence,

to take calculated risks on the basis of sincere risk assessments.

Companies have work to do.

But so do regulators. We, just like Paul here in Gibraltar and Alain and his colleagues in the UK ICO, are working hard to be ready and accountable for our new responsibilities as DPAs.

And Member States of the EU also have work to do.

It is remarkable that so far - with just three months to go - only two Member States have been able to adopt laws updating their data protection laws in the light of the GDPR.

2018 is also very important because there are also two items of unfinished business for the EU legislator.

The ePrivacy Regulation, which is intended to change the incentives in the market away from the constant and covert tracking model.

And the 'GDPR for EU institutions' - a Regulation which applies the same standards and obligations to EU public sector as for private companies.

Then of course there is the question of Brexit. It is an enormous question for people in Gibraltar, and I would like to conclude my opening remarks on this subject.

Brexit is a big disappointment to everyone who believes in the EU and being united in diversity.

But in building global partnerships, the UK post-Brexit would be an obvious close partner.

We are not involved in any negotiations, which are of course highly politicised.

I have seen the UK's statements of commitment to the free flow of data and ongoing regulatory cooperation.

The EU data protection laws, GDPR included, should apply to in the UK before the withdrawal date.

From midnight 30 March 2019 the UK and by extension Gibraltar will become a "third country" for the purposes of EU law - unless there is a unanimous agreement of the Council to extend the deadline or agreement to a transitional period.

Some UK business will continue to live a full life under the GDPR by virtue of the Regulation's extra-territorial reach.

For others, the situation will depend on the agreed future relationship.

If UK remains party to EEA Agreement and therefore in the Single Market, the GDPR would continue to be directly applicable to the UK (though it would be free to choose whether to continue to transpose police Directive 2016/680 into EU law). This scenario appears to have been categorically rejected by the current UK Government.

If the UK were admitted as a member of EFTA but not part of EEA, UK would need to apply for adequacy under GDPR.

Without adequacy, data transfers would require other grounds provided for in the GDPR.

So, by and large, any of discussed models presuppose a certain degree of, if not full, implementation of or compliance with the GDPR.

Overall, Brexit or no Brexit, Hard Brexit or Soft Brexit, Quick Brexit or Slow Brexit - data flows, like supply chains, will still be global.

The UK has a unique interest in smooth data flows - not least because of the importance of its financial sector.

We shall see what will happen in the coming months.

The adequacy exercise in effect has shone a light on dark practices which are of concern to all champions of fundamental rights.

Thanks to the Court of Justice of the European Union in the Schrems judgment on the Safe Harbour adequacy decision, we know that the EU standard is now clearly incompatible with indiscriminate access to personal data for vague security purposes.

I remain stubbornly optimistic that Brexit will not happen in the end.

But if I am wrong, perhaps one good thing will come out of Brexit and an adequacy application.

It will provide a further opportunity to clarify the boundaries of legitimate and proportionate spying activities in a democratic society.

Thank you for your attention and I look forward to our discussion.