**Europe's big data protection opportunity**

**Keynote address to the Banking and Payments Federation, Ireland**

**8 October**

***Giovanni Buttarelli***

***European Data Protection Supervisor***

Thank you to the Banking and Payments Federation Ireland for the invitation to be with you today.

The Data Protection Commissioner has just delivered a comprehensive overview of the challenges here in Ireland for data protection generally and in the banking and payments sector specifically. And she has eloquently situated these challenges within the European and global context.

Before giving you a view from Brussels, allow me to share some experiences as someone who has led for several years a national data protection authority.

I fully agree that professionalism in providing a service to the public, with data protection compliance an integral part of good administration, is equally necessary whether we speak of common law or civil code traditions.

From day one, when I took up post as Secretary General of the Italian data protection authority in 1997, I had to deal with important cases in the finance and banking sector:

- the mandatory collection of data by the Italian national bank as part of a register of high level exposure to impropriety
- e-banking security
- ex officio prosecution of computer related crimes
- the kind of data to be retained for at least 10 years because of anti money laundering legislation
- the way in which consent for processing personal data, including sensitive data, was obtained for contractual purposes
- the activities of call centres based on profiling of customers
- the unjustified disclosure of data to lawyers or private investigators for purposes of legal defence.

I will first discuss our vision and strategy for data protection in the generation to come.

I will turn then to the EU's General Data Protection Regulation, whose negotiations are nearing conclusion.

And finally I will touch on some issues more specifically relevant to big data in the banking sector.

The EDPS remains a small institution - around fifty employees. I am responsible for ensuring compliance of the EU institutions with data protection rules. And we also have a remit of advising the EU bodies, like the Commission, Parliament and Council, on all matters affecting fundamental rights, in particular the rights to privacy and to data protection.

The assistant EDPS, Wojciech Wiewiorowski, and I published a strategy within 100 days of our mandate. Our vision is for the EU, and particularly Member States with a dynamic tech sector like Ireland, to lead by example. We want the EU to develop a new approach to data protection, which holds true to data protection principles at the same time as embracing the benefits of technology.

This means less prescriptive rules – leaving the detail of how to comply with the rules to businesses.

It means, instead, more accountability for how personal information is treated.

We ask the legislators to do less.

We ask the controllers and independent regulators to do more.

And it means more openness in telling individuals what is happening to their data, and allowing them to take more control over it.

Instantaneous, international data flows are a reality.

That is an opportunity for the EU to build partnerships across the world, based on common values.

The judgment from the European Court of Justice on Tuesday gives us a chance to build not a new harbor but a bridge, constructed from both sides, EU and US, built from reciprocal respect, reciprocal rights for all whose data is processed.

To borrow the environmental call to action: the data protection authorities and responsible controllers needs to **act local and think global.**

But this is not just about compliance with the law.

We have to think about the long term implications for society of big data, internet of things, artificial intelligence, self-driving cars and other frontier technologies.

So I am trying to promote an ethical underpinning to this great project. For more information you may like to read our recent Opinion on digital ethics and technology, published in September.

**Let me now address the reform of the data protection rules in the EU.**

In July we published – in a free-to-download app – recommendations on improving each article of the General Data Protection Regulation.

We have three big objectives in our policy intervention:

- a better deal for citizens

- rules which will work in practice
- rules which will last a generation

The reform should reverse the recent trend towards secret tracking and decision making on the basis of profiles hidden from the individual.

The problem is not targeted advertising or the practice of profiling, but rather the lack of meaningful information about the algorithmic logic which develops these profiles and has an effect on the data subject.

We recommend fuller transparency from controllers.

We strongly support the introduction of the principles of data protection by design and by default as a means of kickstarting market-driven solutions in the digital economy.

We recommend simpler wording for requiring the rights and interests of the individual to be integrated in product development and default settings.

And we want the reform to empower individuals.

For example, data portability is the gateway in the digital environment to the user control which individuals are now realising they lack. We recommend allowing a direct transfer of data from one controller to another on the data subject's request and entitling data subjects to receive a copy of the data which they themselves can transfer to another controller.

We recommend avoiding language and practices that are likely to become outdated or disputable The EU's data protection authorities should be ready to exercise their roles the moment the GDPR enters into force, with the European Data Protection Board fully operational as soon as the Regulation becomes applicable.

Authorities should be able to hear and to investigate complaints and claims brought by data subjects or bodies, organisations and associations.

Documentation should be a means not an end to compliance; the reform must focus on results.

We recommend a scalable approach which reduces documentation obligations on controllers into single policy on how it will comply with the regulation taking into account the risks, with compliance demonstrated transparently, whether for transfers, contracts with processors or breach notifications.

What is the relevance of all this for the banking and payments sector?

We published a year ago some sector-specific guidelines on how lawmakers can integrate privacy and data protection into financial services regulation.[1] We have been proactive in advising new EU regulatory bodies on how to exercise investigative powers in line with data protection rules, and to require banks and financial institutions to provide only the personal information which is necessary and relevant.

[1] EDPS Guidelines on data protection in EU financial services regulation, 26 November 2014. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Thematic%20Guidelines/14-11-25_Financial_Guidelines_EN.pdf

But this is a dynamic sector, and there is great excitement over the potential exploitation of 'big data' analytics.

So allow me to spend some time addressing this question.

And regulators are now taking an interest – as seen with the announcement on Monday this week of a joint investigation in the risks and benefits of big data by the European Banking Authority, European Securities and Markets Authority, and European Insurance and Occupational Pensions Authority.

In May, the European Commission published a communication on the Digital Single Market.

'Big data, cloud services and the Internet of Things,' it states, 'are central to the EU's competitiveness.' One of the proposals we are told to expect will aim to remove unjustified restrictions on the 'free flow of data' within the EU including 'questions of ownership, interoperability, usability and access to data in situations such as business-to-business, business to consumer, machine generated and machine-to-machine data.'

This echoes the G8´s 2013 Open Data Charter whose principle of ´open by default´ aims to make data more freely and openly re-usable.

This is not a new paradigm.

If the processing becomes more complex, data controllers have the responsibility to ensure users and consumers are properly informed.

Previous generations of data protection rules have addressed the transition manual to automated processing, from analogue to digital networks, from the pioneering development of e-commerce to the Information Society, from silos to interconnected large-scale data systems.

Fundamentally this is a question of scale.

We have argued that Big Data - used well - can be used to change the world positively without compromising our fundamental rights.

Technology has changed the nature of personal data. It used to be a question of the data we gave controllers. But now, with profiling, companies have data about us which we never had, as data subjects and which we don't know anything about.

How can an individual control or understand these developments?

There is the widely reported story of the perfectly solvent media professional in the US who returned from holiday to find that their credit card limit had been drastically reduced because they'd been shopping in stores where customers tend to have bad repayment record.

This limit was reduced with an algorithm.

So fairness and transparency are key features of data protection law and the Charter of Fundamental Rights.

But these algorithms tend to be hidden.

Are they 'fair'?

According to a book published this year by Frank Pasquale, credit scoring is the original 'black box':

In 1960s banks had undercover investigators who would mark down borrowers if they had untidy backyards or 'effeminate gestures'.

Now these firms are regulated and the rough outlines of the scoring process is known.

But in the future the Internet of Things could enable detailed knowledge of a life in the most intimate places.

And big data allows all sort of combinations from the 'digital breadcrumbs' we all leave not just with credit cards but in social media, travelling around with contactless public transport smartcards, wearable devices.

Social media reveals what sort of friends you have, perhaps your political views and sexual orientation, how you spend your leisure time: potentially very interesting information for a risk-conscious institution.

It's illegal to discriminate on gender or race grounds, but how can you tell if the algorithm is hidden?

What will be the impact on society and individuals?

The US National Consumer Law Center found that credit products sold on the basis of non-traditional data-led processes offered annual percentage rates of between 134% and 748%!

So this is an excellent area for exploring the opportunities and pitfalls of new technologies in service provision.

I am no longer responsible for the direct supervision of private entities.

But a number of principles, which I know the Irish Data Protection Commissioner shares, might be valuable in considering how to be fully accountable with the GDPR in force:

- data minimisation, and avoiding creating unnecessary databases that create security risks.
- transparency about data protection policies and procedures, including what actions need to happen in the event of a data breach.
- considering what breaches might do harm to customers and pay particular attention to mitigating these risks – in relation to the susceptibility of the data eg what could be subject to fraud, such as passport details.
- considering how to allow individuals to access and port their personal data to other providers.
- investing seriously in data security.

Let me conclude with one excellent piece of advice I saw on the site of a financial services blogger: 'Customers should be treated as a source of business rather than a piece of data and need to be treated fairly, with respect to their rights to privacy and without cynicism.'[2]

The *Schrems* case for me highlighted the centrality of respect for human dignity in all the frenzied debates about privacy and data protection.

I've delighted to have had the chance to be part of this conference.

Thank you for listening. I look forward to our discussion this morning.

[2] http://techcitynews.com/2015/05/01/eus-general-data-protection-regulation-poses-the-biggest-threat-to-business-continuity-for-a-decade/