Application of Data Protection rules in relation to financial services and the digital economy

Speech at BBA's Data Protection & Privacy Conference

British Banker's Association, London, 15 September 2016

Giovanni Buttarelli

Ladies and gentlemen,

First of all, let me thank Anna, Helen and the BBA for your invitation. I am very glad to be here and to have the opportunity to share with you a few considerations on the way data protection is evolving, particularly in the financial services industry, a sector that has proved innovative and dynamic in looking for new business opportunities after the crisis.

In starting our conversation on this topic, we shall bear in mind what - I believe - are interesting trends in today´s economy: the increase in the use of big data, the globalisation of capital and financial services and the "credit crunch" generated by the economic crisis, with the need to know more about customers.

I am mentioning these trends as they are inspiring the most recent actions by the legislator and the sector regulators and, as a consequence, the most crucial challenges for us at the EDPS. It is part of our mandate, in fact, to assist the legislator in adopting new legislation ensuring, at the same time, that the new rules embed solid data protection safeguards and do not limit individual rights more than it is necessary and acceptable.

If you permit me to draw an analogy:

If financial services are the engine of the modern economy and liquidity is the fuel, then regulation should be the lubricant that keeps the engine from stalling. And this sector more than any has

profound experience of regulation and need to demonstrate compliance and accountability.

But I would pursue the metaphor further: personal information is more than ever the raw material used to produce the engine itself.

Personal data, big data, has become the indispensable element for identifying opportunities in the market, and not just in banking and financial services.

In this respect, there is a question I would like to pose to you. How should we consider data protection in today´s society? What is its dimension as an individual right? What its relevance compared to other interests being affirmed in our world?

As to the first question, we know that privacy and data protection are fundamental rights based on Article 8 of the European Convention of Human Rights and on Articles 7 and 8 of the EU Charter of fundamental freedoms.

Data protection, as a fundamental right, helps human beings to preserve their position and their dignity in society, even as society changes and evolves, and to grow and evolve themselves.

As to the relevance of data protection in the contemporary world, I often hear the routine argument that regulation (not only data protection, to be frank) stifles innovation and hampers the development of markets. This argument describes the dynamics of over-regulated markets, which suffer from byzantine bureaucracy, but this is not the world we live in today, not the world we have in mind as data protection regulators.

The vision we have in mind at the EDPS is one where markets develop and innovate in a rapid and dynamic way, following the intuitions of entrepreneurs and the desires of people. These markets need the solid foundations of responsive and non-invasive regulation.

We often see timely regulatory interventions happen. In the United States, for example, after the *Enron* and *Worldcom*

scandals in 2001, the legislator enacted section 404 of the *Sarbanes-Oxley Act*, in order to make managers of listed companies directly accountable for the financial statements disclosed to the market. Of course, these measures increased compliance obligations, but they also helped restore people´s trust in financial markets and contributed to new investments and growth.

As we have learned the hard way from the financial crisis, markets, once left to themselves, may fail, sometimes hurting the most vulnerable among us. Only good regulation, will prevent such failures. That is why, beginning from 2012, we have devoted significant efforts and resources to contribute to the reform of EU data protection rules, in the form of a general regulation directly applicable in the entire European Union.

The new General Data Protection Regulation is entering into force in May 2018, but, already now, we are witnessing a transition from the system of the Data Protection Directive to the

GDPR. The Directive provided a general legal framework that has worked well for over 20 years but is of course out of date in several ways. The GDPR fills the gaps that economic, social and technological developments have created and brings data protection up to speed with the current society. Of course, this means changes we all need to adapt to.

The GDPR does not contains specific provisions dedicated to financial services, but changes will happen also in this industry. In particular, the GDPR raises the bar of accountability: if you want to improve your business performance by processing personal data and big data, you are welcome to do it, but you have to take responsibility and become more proactive and more "data protection literate", in order to do it.

For example, if you want to profile your customers´ personal data for direct marketing purposes, they need to be informed and have the right to object. Similarly, if you want to develop an online loan website that automatically selects the customers who should

receive a loan, the customers accessing such website shall be informed of the existence and functioning of the automated evaluation system. They have the right not to be subject to automated decision or, when exceptions apply, at least the right to obtain human intervention on the part of the controller, to express their point of view and to contest the decision.

Also, the GDPR has consolidated into law the principles of *privacy-by-design* and *privacy-by-default*, with the result that data protection safeguards will have to be built in the system used to process personal data and will have to apply as default options, in case data subjects does not express their own choice.

As you can see from these few examples, the GDPR entails more responsibilities for those who engage in data processing. I consider, at the same time, that this a necessary step in today´s high-tech economy and that the GDPR efficiently places responsibilities on those with the broadest shoulders.

The GDPR is a comprehensive and articulated piece of legislation, which aims at improving and harmonising data protection throughout Europe. I can cite the one-stop principle, that ensures that data protection issues that affect multiple jurisdictions are effectively handled under the lead of a single authority. I can also refer to the consistency mechanism, which ensures that the data protection rules are interpreted and implemented consistently in all Member States, thus *de facto* ending the season of forum shopping. In this context, I shall not forget the crucial role of the EDPB, which will take over the functions of the Art. 29 WP and ensure consistency in the application and development of data protection law.

Having the privilege of addressing this audience and having mentioned the contribution of the EDPS to the adoption of new legislation, I would like to mention recent advice we have provided in this respect.

A major field of work has been the anti-money laundering Directive, recently entered into force, which has been the subject of several amendments (some still in the process of being approved), aiming at fighting terrorism financing, tax evasion and illegal business.

Such legislative initiatives are important to fight criminality, restore legality in the financial system and support economic growth. We have been consulted during the adoption process and have contributed with advice on how to implement effective data protection safeguards in that delicate context.

Contrary to those who consider data protection as an obstacle to the deployment of important and urgent public policies, I expect that our work will allow the optimal operation of these policies, avoiding, for example, that the anti-money laundering Directive is annulled in Court as it was the case for the data retention Directive in the *Digital Rights Ireland* case. In this respect, we are enablers, not censors!

In opening my speech, I also referred to the reduction in the availability of credit to households and enterprises. Who, among us, has not heard the claim that business cannot invest and recover from the crisis due to lack of credit from the banks?

Extending credit entails an assumption of risk by a financial institution. The availability of data, including personal data, allows a better assessment of such risk, with the effect that it is easier for banks to spot potentially insolvent debtors and channel resources towards debtors with a better record of repaying their debts. In this context, big data enables banks to better assess the risk they face and, overall, the credit market might work more efficiently, but what about citizens and customers? Will they be taken care of?

Big data enhances banks´ risk assessment capabilities. It also improves the transparency of the market, but only in a direction: from the perspective of financial institutions, which sees and knows more about their customers. We are concerned that

customers have the opportunity to access the personal data that banks store about them, that they are able to verify that such data are correct and that, ultimately, they are allowed to interact with the bank in the assessment of their credit risk, rather than remaining passive. This is even more necessary, as big data relies on algorithms and economic models that operate always in the same way, perpetuate assumptions (or biases) and may cause distortion to the detriment of citizens.

For the reasons I have just described, to ensure that the credit market operates in a fair and transparent manner, we are partnering with financial institutions and regulators, in order to understand how data protection safeguards should apply in the banking industry, whether and how customer information collected for regulatory purposes (*e.g.* anti-money laundering) can be used for secondary purposes such as creditworthiness assessment and even for commercial and promotional uses. Considering that there is a large demand for personal data for all

purposes, we aim at establishing a "safe platform" for citizens, enabling them to remain in control of their data whenever they engage into market transactions in their day-to-day life.

My reference to a “safe platform” certainly brings to your mind the negotiation and approval of the “Privacy Shield”, which replaces the Safe Harbour decision.

Like its predecessor, the GDPR provides for different ways to transfer personal data from the EU. The “Privacy Shield” is one of the so-called “adequacy decisions”, whereby the European Commission decides that a third country provides for an adequate level of protection and can therefore be recipient of personal data sent from the EU. In the absence of such a decision, other means such as contracts or binding corporate rules can be used to legally transfer the data.

This summer EU Justice Commissioner Věra Jourová and U.S. Secretary of Commerce Penny Pritzker announced the new framework for transfers from the EU to organisations in the U.S.

that may certify under the Privacy Shield. The Commission adequacy decision adopted in July is based on this framework. Adequacy decisions, as general solutions for transfers from the EU, are welcomed. But experience shows us that they have to be comprehensive and solid enough to last and provide legal certainty to individuals and organisations in the long term. To continue on the international scene, I would like to mention efforts to modernise the Council of Europe Convention on personal data protection, an antecedent of the EU framework. This Convention has a universal vocation and is now being updated. Countries from all continents enacting new data protection rules are now applying for accession.

The work of EU data protection authorities with APEC economies to guide companies willing to transfer data also shows how the protection of personal data does not prevent, but facilitates the transfer of information in a legal, secure and trustful environment.

Ladies and gentlemen,.

I would like to pay tribute to the BBA for organising this important conference.

I hope that this provides the opportunity for representatives of this vital industry to lead by example, show true accountability in compliance with the new data rules. I am delighted to have had the chance to be part of this event.

Thank you for listening. I look forward to hearing your questions.