**Cybersecurity and Privacy Innovation Forum 2015**

Brussels, 28 April 2015

**Keynote address**

*Giovanni Buttarelli*
*European Data Protection Supervisor*



Ladies and gentlemen,

Let me first thank the organisers for inviting me to speak to you today.

You may be aware that last month I published my five year strategy, and reinforcing the rights to privacy and data protection in cyberspace is central to my priorities. So this year's Cybersecurity and Privacy Innovation Forum is timed perfectly, and it gives me my first opportunity to address this issue..

For me, as European Data Protection Supervisor, I cannot overstate the importance of technical development and research work on privacy and data protection.

Our strategy lays down three big objectives:

- We want to take data protection fully into the digital age and digital markets
- We want to forge new and effective global partnerships, and
- We want the EU to open a new chapter for data protection

The first objective refers to the need for better technologies that enhance privacy and data protection:

- that means policy solutions that go across the borders of disciplines

- it means increasing transparency of data processing, giving users more control about the processing of their data

- and it means strengthening the concept of accountability in big data processing.

So I am very pleased that this conference is focusing on technological innovation relevant to both cyber security and privacy.

One of the tangible contributions to these discussions is the Internet Privacy Engineering Network – IPEN – which we established last year together with other data protection authorities and partners from industry, academia and civil society. It brings together different disciplines and developers from different areas to work together on implementing practical privacy.

I welcome the IPEN participants who are here today.

A presentation of the network will be held this afternoon by my colleagues, and a side workshop is also scheduled.

But we must also look at the bigger picture of cyber security, and consider the implications at a broader scale.

## Cyber security poses challenges at technical and policy level:

**At the technical level**, Cyber-security is key to the sustainability of our digitally supported economy and society.

Cyber security serves to prevent and respond to cyber disruptions and attacks.

There will be plenty of presentations on the technological aspects at this conference, so I will leave it to the many experts assembled here to deepen our knowledge of this area.

**At the policy level**, cyber-security requires collaborative effort to tackle all threats which are the unfortunate by-product of our interconnected world.

The security of our networks and services depends not only on the measures we take for our own infrastructure, but also on those addressing the security of the infrastructure to which we are connected.

What is needed is a high common level of network and information security to ensure effective security across the board, including all EU actors and EU institutions.

With today's global interconnectedness, cyber-security has an international dimension which goes beyond the EU borders.

## So let me make a few remarks about the need for collaboration.

This international dimension makes an effective cyber-security policy a big challenge

Indeed, threats can affect organisation around the globe at the same time, including compromises of personal data.

But this international dimension can be leveraged and create opportunities to work together, to work together more efficiently, more holistically.

Threats and vulnerabilities in one organisation, if communicated properly to partners, can be dealt with quickly and thoroughly thereby ensuring the protection of all systems and all data processed on those systems.

There is a strong need for collaboration between stakeholders so as to ensure that the cyber-security issues are dealt with as efficiently as possible.

Collective risk requires collective responsibility.

But who are the stakeholders in this cyber-security context? Industry, academics, policy makers and business investors such as the people in this audience of course…

But other groups are also interested in this field as it has an impact on their specific area of expertise.

The field of privacy and data protection is one of those areas.

We have to strive for reconciling the different rights and interests at stake.

The rights to privacy and data protection have long been perceived as conflicting with the objective of cyber-security. I believe that this is a misperception.

A basis for this international cooperation was laid down with the Budapest Convention on Cybercrime which was established in 2001 and has in the meantime been ratified by 45 countries, not only in European countries but also others including the US and Australia. This convention provides a basis for cooperation in fight against cybercrime based on respect for fundamental rights.

**This provides guidance for our work on cyber security in general.**

The EDPS believes that measures for ensuring a high level of cyber-security should help improve the security of all the information processed, including personal data. Security of data processing has always been a crucial element of data protection.

Work on cyber-security can thus play a fundamental role in contributing to ensuring the protection of individuals' rights to privacy and data protection in online and networked environments.

That said, the objective of cyber security may be misused to justify measures which weaken protection of these rights.

With more and more personal data being processed through information systems and networks, cyber-security must not become an excuse for disproportionate processing of personal data.

We need to find the right balance, and data protection principles like necessity and proportionality can help guide the design of privacy by design and by default cyber security solutions.

As EDPS, I will continue to advocate a constructive approach. Such as when we contributed to the setting up the Cyber Crime Centre, to the EU cyber security strategy and the Network and Information Security Directive.

## Policy and Technology cannot be separated

Negotiations on reform of the EU's data protection rules are, we hope, entering their final stages. A key plank of this reform is data security.

According to the current Data Protection Directive, three elements determine the selection of technical and organisational measures:

- The risk of the processing
- The state of the art, and
- The cost of the measures.

The former two must clearly be maintained. For the third element, we must be careful not to overstate the costs of appropriate data security.

We should note that not all Member States have transposed this clause in their national laws implementing the current Directive - including I'm afraid my own country. Italy.

A proper cost benefit analysis would demonstrate that data security benefits not only individuals whose personal information is processed, but also the professional reputation of the organisation processing the data.

Let's not forget that when the European Court of Justice last year found the Data Retention Directive to be invalid, one of the reasons was concern about the inadequacy of the data security provisions in the directive.

Some have interpreted the judgment as implicitly advocating a stricter determination of the storage location.

I disagree.

Physical location is not the determining factor in security. Rather it is degree of control, accountability and responsibility which data controllers demonstrate when processing personal information. They must take full responsibility for all the measures they implement, regardless of the technology they use. As we put it in our opinion around the time of the judgment, "responsibility must not vanish in the clouds".

## What are the current challenges for cybersecurity actors?

It is difficult to predict future developments. But we can extrapolate some likely developments from current knowledge and recent experience.

In 2015/2016 I foresee mounting challenges for cybersecurity.

Sectors - like banking and health - that were already the focus of attacks will need to continue shoring up their defences.

We will probably see an increase in politically motivated attacks that seek to disrupt, for example industrial control systems.

We can expect a rise in the capabilities for cyber-attacks of both states and profit-motivated criminal groups. Attacks will become more widespread, affecting more individuals, and more complex. We might even detect an emerging market for these advanced capabilities.

Given the increasing awareness of security related matters, we can expect more and more reported events and more discoveries of vulnerabilities, which will allow the security community to react and fix the issues before they become too damaging.

What we can also expect is more discovered vulnerabilities in older tools which are deployed widely: think for example of the bug in OpenSSL - due to an increasing scrutiny of those tools.

What will remain, maybe unknown to this security community, are the most advanced attacks using difficult-to-find vulnerabilities. These corresponding exploits might be considered very valuable and be traded or sold. These vulnerabilities might be

leveraged as much as possible by attackers seeking to gain long term footholds into corporate and EU institution networks.

With a tighter control on vulnerabilities, we can expect an increase in social engineering attacks in order to gain access to protected resources. This is a field where the best tool we have to defend ourselves and our data is more training and awareness of users.

Other IT fields in which we can anticipate more issues are related to the Internet of Things, Bring Your Own Devices and the ongoing developments in wearables (watches mainly at this stage) which are gaining in popularity and in capabilities. These attacks would have a significant impact on privacy and the protection of personal data.

The good side of the story is that in general, there is more awareness of security issues in the world and more investment in cybersecurity as companies and organisations realise what is at stake

An increasing use of encryption is a further likely result of this increased awareness and ongoing revelations with regards to surveillance activities by states. By-products of this increasing use of encryption, if the encryption mechanisms are implemented properly, may be the need for more sophisticated targeted tools for law enforcement and for scanning and analysing network traffic to study and prevent attacks.

## And what are the challenges for the legislator?

For nearly twenty years now, the EU data protection directive has provided a solid basis for safeguarding the fundamental rights to privacy and data protection. But after so many years of rapid technological and business development, the law is due for maintenance.

We urge the European Parliament and the Council to adopt a new framework which reinforces the rights of the individual, before the end of this year.

Now is not the time to weaken the protection of personal data and to lower the level below the one provided by the current Directive.

We must strengthen the principle of accountability, as I have just mentioned. One tool for reinforcing accountability is the introduction of a general data breach notification obligation, which will force controllers take the necessary organisational and procedural measures. The new rules will create a strong incentive to allocate responsibility for the prevention of such breaches at the appropriate level of the organisation.

Accountability underpins network and information security, including the current model of risk management for security.

The data protection reform will contribute to determining which technological development and research we need in order to implement appropriate safeguards for personal data processing and cyber security. This will provide impulses to the work of the researchers and developers participating in the programmes and projects presented today and tomorrow.

I wish you a successful conference.

Thank you.

- - - - - -