EU-U.S. data flows and data protection: opportunities and challenges in the digital era -- Speech at the Center for Strategic and International Studies by Věra Jourová, Commissioner for Justice, Consumers and Gender Equality --

Washington, 31 March 2017

Ladies and Gentlemen,

Thank you very much for inviting me to speak on the very topical issues of transatlantic data flows and the protection of personal data.

On my previous visit to Washington in 2015, Paris had just been struck by terrorist attacks.

In a rather sad turn of events, here I am again in Washington one week after the attack in London that killed 4 people and left 40 others wounded.

The attack unfolded over Westminster Bridge in the shadow of Big Ben and the Houses of Parliament — the very symbols of democracy.

Democracy, our way of life and our values of tolerance were once again struck at the heart on that day.

The European Union and the United States are united in their resolve to defend our free societies against crime and terrorism. This is why our transatlantic dialogue on these issues is so important.

More than ever, we need to cooperate and protect our respective citizens from common security threats.

But in doing so we need to reconcile security interests and upholding fundamental rights.

[Umbrella Agreement]

One of our common achievements in this respect is the EU-U.S. Umbrella Agreement on protecting personal information exchanged as part of law enforcement cooperation. This includes information on suspects and convicted persons, but also innocent victims and witnesses.

The Umbrella Agreement, which came into force on 1 February this year, is a big improvement compared to the past situation when our information exchanges were subject to fragmented and often weak protections which caused legal uncertainty and exposed them to legal challenges.

With the Umbrella Agreement, we now have a common transatlantic privacy framework based on high standards.

This will support and facilitate law enforcement cooperation by building trust and legal certainty for data transfers.

We can be proud of this achievement, which is also a major precedent and will serve as a model for similar agreements in the area of law enforcement cooperation.

Now that this major agreement has entered into force, we must ensure that it is fully and effectively implemented, on both sides of the Atlantic.

This is something we owe our citizens and their right to privacy, but it is also crucial for effective, rapid and secure law enforcement cooperation.

[E-evidence]

This brings me to my next point on electronic evidence. Today, access to digital evidence often provides the only lead in investigating or prosecuting crime.

If access to e-evidence can be tricky at national level, it is even more so when the data is stored outside of the country of the investigating authorities.

EU Member States are exploring ways of addressing this problem, either through traditional instruments such as mutual legal assistance or alternative tools such as direct requests to companies.

Access to electronic evidence raises many questions, from jurisdictional issues to the protection of personal data. In Europe, among the 28 Justice Ministers there is a growing consensus for a common approach with clear criteria that would also provide legal certainty for business.

I am also fully committed to further pursue our transatlantic dialogue on this topic, both with the Government and internet service providers in the United States.

[Online hate speech]

For all the useful information and opportunities it provides us with, the Internet can also be used as a channel to spread messages of hatred and calls to violence.

Over recent years, racism, xenophobia and other forms of intolerance have been growing and spreading across Europe at very high speed.

The European Union rejects and condemns all forms of intolerance and incitement to hatred and violence: they do not belong in our societies!

I want the Internet to remain a place of free and democratic expression, where the law is respected. The rule of law must apply online, just as it does offline.

In May last year, I agreed with Facebook, Twitter, YouTube and Microsoft on a Code of conduct to counter illegal hate speech online.

These IT companies committed to review and assess most of the notifications of illegal hate speech in less than 24 hours.

We are currently monitoring how the Code is implemented and I expect the results to be released by the end of May.

A lack of progress may challenge the effectiveness of self-regulation in this area and may increase the pressure to legislate.

[General Data Protection Regulation]

Turning back to the protection of personal data, our revised General Data Protection Regulation will come into force in 2018.

These are modern 21st century rules, adapted to the digital age. And we will swap the 28 different set of national laws with one single set of rules for Europe's Digital Single Market. This is good for the protection of the individual and good for innovation and business across the EU, including for American companies doing business in Europe.

We are currently working closely with Member States, with the data protection authorities and with businesses to ensure effective implementation in practice. We need to get this right.

[The Privacy Shield]

This brings me to my last point which is the Privacy Shield.

In a world where cross-border data flows have become a central feature of global trade, strong data protection rules would be meaningless if the data can travel abroad without protections. This applies in the transatlantic context as in any other trading relationship.

At the same time, while the EU and the U.S. both protect privacy and personal data, our approaches in how to safeguard these rights differ in some respects.

The Privacy Shield – like the Umbrella Agreement in the law enforcement area – shows that it is possible to bridge those differences.

I am pleased to see that a growing number of US companies have endorsed this framework.

Almost 2,000 of them have already signed up to the Privacy Shield.

This framework has enormous potential to strengthen the transatlantic economy and reaffirm our shared values.

But we now have to ensure that it keeps working as it should.

Two things are important here.

First, we have to ensure that the key foundations of the Privacy Shield remain in place. This concerns in particular the area of government access for national security reasons.

Maintaining the limitations and safeguards in this area is crucial. For instance, there would be no Privacy Shield without Presidential Policy Directive No 28 and the Ombudsperson. Both are central elements of the representations and commitments on which the framework is built. And we will also follow closely this year's debates around the reform of section 702 FISA and how this will affect the data of Europeans.

And second, we have to ensure the proper day-to-day implementation and robust follow-up of the Privacy Shield.

Companies have to comply with their obligations and this needs to be reflected in their daily operations. And the public authorities that oversee the Privacy Shield, both here and back in Europe, have to monitor such compliance and help individuals exercising their rights.

Yesterday Commerce Secretary Ross and I agreed that the first annual joint review of the Privacy Shield will take place in September this year. This will be an important milestone where we need to check that everything is in place and working well. If we want to further consolidate this new transatlantic bridge, we need the active engagement and contribution of all interested parties to the review.

[Conclusion]

Ladies and Gentlemen,

Transatlantic data flows have come a long way.

The Umbrella Agreement and the Privacy Shield will benefit our citizens and businesses, provided they continue to be properly and fully implemented.

I have come here to engage with my new counterparts in this spirit. I am happy that we have made a positive start this week and reaffirmed our common commitments.

SPEECH/17/826

Press contacts:

Christian WIGAND (+32 2 296 22 53)
Melanie VOIN (+ 32 2 295 86 59)

General public inquiries: Europe Direct by phone 00 800 67 89 10 11 or by email