Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe)

Strasbourg, 26 October 2015

Speech by Commissioner Jourová before the Committee on Civil Liberties, Justice and Home Affairs (Libe)

In the plenary debate on 14 October I referred to the Commission's immediate priorities following the Schrems ruling:

- To reassure our citizens that their personal data will be protected when they are transferred abroad;
- To ensure clarity for European businesses that need to transfer data to the US, about the remaining legal ways of doing so;
- To work together with the national data protection authorities to ensure a coordinated approach and to avoid fragmentation in the internal market.

I also announced that the Commission will step up talks with the US towards a renewed and sound framework for transatlantic data flows. And I stressed that I want to work on this together with you, in partnership and transparency.

Let me today update you on the latest developments. And I also hope to hear from you on how you can support this process, especially in the run-up to my visit to Washington in mid-November.

Since the plenary debate on 14 October the Commission has been working closely with the European data protection authorities (DPAs) in the Article 29 Working Party. The important role of these independent Data Protection Authorities has been emphasized by the Court.

On Friday, 16th October, the Art 29 Working Party issued a statement on the consequences of the judgment. Notably, the Working Party referred to the ongoing negotiations on the revision of Safe Harbour as an important element of how to address the present situation, calling on the EU institutions to find ways to enable data transfers to the United States that respect fundamental rights.

As to the current business activities requiring personal data transfers, the Working Party confirmed that other available tools, such as Standard Contractual Clauses and Binding Corporate Rules, can still be used, even though the Data Protection Authorities will further analyse the possible impact of the judgment on these alternative tools.

The Working Party announced that if, by the end of January 2016, no appropriate solution is found with the US authorities and depending on the outcome of the assessment of the alternative

tools, EU Data Protection Authorities would take all necessary and appropriate steps, including enforcement action.

While we welcome the Working Party's support for a new transatlantic framework by January 2016, the Commission also feels strongly that business need maximum clarity in the meantime.

When I met business and industry representatives together with VP Ansip and Commissioner Oettinger on 14 October it was clear that they were looking for clear explanations and a uniform interpretation of the ruling.

The Commission will therefore soon issue an explanatory Communication on the consequences of the *Schrems* ruling setting out guidance on international data transfers. However, this cannot – and must not – replace the work of the Data Protection authorities in upholding and enforcing data protection rules. The Commission will continue to support their work in ensuring that a uniform approach is taken in the framework of the Article 29 Working Party.

[On the negotiations with the US]

Given that the Safe Harbour was one of the central avenues for data transfers from Europe to the U.S., it is crucial to conclude the discussions with our U.S. counterparts on a renewed framework for transatlantic data flows with a higher level of protection. This is important for transatlantic commercial relations and for our citizens.

We need to make sure that the new arrangement lives up to the standard of the Schrems ruling.

Already prior to the judgment, the Commission identified a number of issues that in its view needed to be addressed in a revised Safe Harbour, in its 13 Recommendations of 2013.

In light of the Court's judgment we need more clarifications from our U.S. counterparts on a number of points. And we have not been dragging our feet: We have immediately resumed discussions with our American counterparts and already had several meetings at technical level. I spoke again with Commerce Secretary Pritzker earlier today to take stock. For the coming weeks, intensive technical discussions will continue and we have agreed to be in regular contact before I go to Washington in mid-November. These discussions are not easy, but I am confident that by then we should already have seen progress.

Let me spell out in more detail what the implications of the ruling are and how I believe they should be addressed.

First to mention is that the Court does not call into question the Commission's power to take adequacy decisions. Rather it clarifies, firstly, the possibilities for data protection authorities to intervene in case of complaints (such as that of Mr Schrems) and, secondly, that the level of protection in the third country must be "not necessarily identical" but "essentially equivalent" to that in the EU.

Let me borrow from the words of the newly elected President of the Court of Justice, Koen Lenaerts, who has explained that the Court was **not**assessing the U.S. system, including their

national intelligence activities. Rather, it was "*judging the requirements of EU law in terms of the conditions to transfer data to third countries, whatever they may be*".

The judgment does not require "*an identity of organization*" of the U.S. legal system, but rather that when it comes to data transfers, it has to offer safeguards which are "*globally equivalent*" to the ones we have in Europe. This is what I am seeking in our discussions with the US.

Secondly, the Court says that a system based on 'self-certification' such as the Safe Harbour is acceptable provided there are "*effective detection and supervision mechanisms*". This has indeed been one of the key elements we have been working on with our US counterparts and already flows from our November 2013 recommendations, notably Recommendations 1 to 11 on transparency, enforcement and redress. The US has delivered on this by committing to a stronger oversight by the Department of Commerce (DoC), stronger cooperation with European DPAs and priority treatment of complaints by the Federal Trade Commission (FTC). This will transform the system from a purely self-regulating one to an oversight system that is more responsive as well as pro-active and back-up by significant enforcement, including sanctions.

This is also why we want our own national data protection authorities to have a more active and visible role in the system than previously was the case. For instance, we have worked on improving the interface and communication channels between DPAs and the DoC. The DPAs will also have a role to play in the review of the functioning of the system.

There is agreement on these matters in principle, but we are still discussing how to ensure that these commitments are binding enough to fully meet the requirements of the Court.

Thirdly, the Court has confirmed that an adequacy decision is a living document; it must be periodically reviewed in light of developments of the foreign system. We are working precisely on this point with the US to put into place an annual joint review mechanism that will cover allaspects of the functioning of the new framework, including the use of exemptions for law enforcement and national security grounds, and that will include the relevant authorities from both sides.

Finally, when it comes to the intervention of public authorities, in particular for reasons of law enforcement and national security, the Court underlines that such access must be subject to clear conditions and limitations. Again, this closely reflects the Commission's recommendation made two years ago. And we are working hard with the US to do just that: to ensure that there are sufficient limitations and safeguards in place to prevent access or use of personal data on a "generalised basis" and to ensure that there is sufficient judicial control over such activities.

Let us be clear about this last point: this is the biggest challenge in the judgment. But let us not forget that a debate on these issues has been taking place also on the other side of the Atlantic. Following the initial surveillance revelations two years ago, which gave rise to the facts of the court case, the U.S. has undergone a period of internal review as regards its national intelligence activities. This has led to reform steps such as the USA Freedom Act, but also the President's

instructions to the whole intelligence community (the so-called Presidential Policy Directive28) on surveillance and the need to take account of privacy rights of non-Americans.

We have already seen some progress compared to the past in the direction of more targeted and tailored surveillance. Moreover, as for the use of data that have been collected, certain protections formerly reserved only to US persons have been extended to EU citizens, for instance as regards further dissemination or the period of retention. We are still in the process of assessing these safeguards and of getting further clarifications, but I certainly see some relevant and encouraging elements there.

In parallel, an important initiative has been brought underway to extend judicial protection under the U.S. Privacy Act to EU citizens. The respective Bill on Judicial Redress has now been approved by the House of Representatives and will soon be tabled on the Senate floor. Once it has become effective, as we expect it will, it would be another important step in guaranteeing protection for data transfers.

We now need to focus on these and other elements and to carefully analyse the extent to which they meet the requirements of the judgment.

Honourable Members, I once again appeal to your strong sense of commitment and engagement to help us in this important endeavour. I want to thank you for the support you provided so far in the context of the Judicial Redress Bill. I would repeat my call to you, as Parliamentarians, to also engage with your counterparts in the US on this issue, be it in Congress or in the Administration, and to be a partner in this. We need your help and that of businesses to convince the US of the necessary further steps.

A successful outcome is very important for our wider relationship with the US, our key strategic partner both politically and economically.

As I said before the plenary, I want a more informed debate about this process and see you as an essential partner in this process. I will keep you regularly informed about the next stages of these discussions.

Data Protection Reform

The *Schrems* ruling reaffirms the importance of data protection as a fundamental right in the EU. It should therefore also act as a reminder to swiftly finalise the ongoing trilogies on the data protection reform.

Important progress has been achieved, and I want to thank you for your work on this. I remain optimistic that trilogues on the **General Data Protection Regulation** can be concluded before the end of 2015 thanks to the combined efforts of the EP negotiators and the Luxembourg Presidency of the Council.

The finalisation of the Data Protection Reform is a key enabler for the Digital Single Market to take off. The new rules will foster a virtuous circle between the protection of a fundamental right, consumer

trust and economic growth.

I am confident that the agreements reached in trilogues will ensure the effective protection of individuals as regards their personal data, and equip businesses to take full advantage of the opportunities of the digital economy.

Let me underline again that the level of protection in our 1995 Data Protection Directive is the very minimum that needs to be guaranteed in this reform exercise.

Let me also indicate that, as regards the interaction between the Schrems judgement and the Regulation, a number of elements of the judgment have already been anticipated in the Regulation (e.g. strengthening the powers of supervisory authorities and more systematic and periodic review of adequacy decisions).

In line with the package approach the Council has reached earlier this month a general approach on the **Police Directive** allowing the starting of trilogues tomorrow.

This important instrument is also a crucial part of the European Agenda on Security, as common rules on data protection will enable law enforcement and judicial authorities to cooperate more effectively with each other.

The EU will therefore be equipped with modernised, clear, and robust rules that will be beneficial for individuals, as well as for the business and public sector. In this way, the EU will remain the standard setter in terms of data protection.

SPEECH/15/5916