Personal data in international treaties and agreements - Privacy Shield

Télécom ParisTech, Friday 6 Jan 2017

1. Introduction

It is a pleasure to be here with so many experts in the field to discuss this highly important issue.

The European Parliament has been consistent in its scrutiny of the Privacy Shield and in calling for a stronger arrangement that provides a level personal data protection, which meets the requirements of the Charter of Fundamental Rights and the Data Protection legal framework. That the agreement is now facing an uncertain future due to the legal challenges against it is something the Parliament warned against in our resolution of 25 April 2016, which called for the implementation of the recommendations of the EU Data Protection Authorities (Article 29 Working Party and the EDPS) to make it a stronger instrument.

Both citizens and tech companies need the certainty of a robust legal framework. However, the election of Donald Trump in the US means that we must now be especially vigilant to ensure that protection standards are upheld and that the agreement is correctly implemented. In addition to this, the Privacy Shield has attracted two legal challenges[1], which, *at best*, raise concern among the hundreds of companies that have already signed up to the new scheme, and, *at worst*, could undermine the entire agreement if either legal challenge succeeds.

With over 500 companies having already certified to the agreement, including Microsoft and Cisco, and a further 1750 having applied, the need for this agreement to meet the legal requirements of EU data protection law is more

[1] Privacy advocates Digital Rights Ireland (DRI) lodged a challenge with the General Court of the European Union in October claiming Privacy Shield does not sufficiently protect the personal data of EU citizens.

Three French organizations, privacy group La Quadrature du Net, non-profit ISP French Data Network and ISP industry association Federation, have also brought actions in the General Court. The French groups argue that the US Ombudsperson, who is responsible for handling EU complaints about surveillance in the US, is not an effective mechanism for dealing with complaints and that the ombudsperson lacks sufficient independence.

pressing than ever. The LIBE Committee has now decided to work on a further Parliamentary resolution as many of the Parliament's concerns remain. We do not have the power to veto the agreement, but the resolution will express many of the serious concerns we have with the Privacy Shield.

The resolution is one of the means at the Parliament's disposal as we continue to pressure the European Commission to take measures (particularly in the joint annual review in **July 2017**) to ensure that the arrangement provides a protection of personal data which meets the requirements of the Charter of Fundamental Rights and the Data Protection legal framework (which will apply from **16 May 2018**).

LIBE delegation: We will also raise these issues with our US counterparts when the LIBE Committee will participate in a delegation to the United States this year from **17-21 July 2017,** when the US Congress and the Senate will be in session. This will follow up on our delegation in **May 2016**, during which several members of the LIBE Committee sought information in particular about judicial redress for EU citizens and the Ombudsperson mechanism under the Privacy Shield. This included a meeting with Catherine A. Novelli, who will take up the role of Ombudsperson in charge of investigating EU citizens' privacy complaints within the US State Department.

2. The Parliament's position

Since the invalidation of the Safe Harbour framework last October, the European Parliament has consistently called for a stronger arrangement, one that provides a protection of personal data which meets the requirements of the Charter of Fundamental Rights and the Data Protection legal framework.

The Parliament considers that international data transfers are essential for economic growth and consumer trust. But they also must be built on solid and strong instruments establishing legal certainty and respecting fundamental rights. In any case, EU data protection law is based on the principle of the continuity of the protection, which means that the level of protection of personal data ensured in the EU must remain when the data are transferred outside the Union. Otherwise, the system would be easily circumvented.

The ruling of the ECJ on the Schrems case sets out clear indications on the basic principles to respect in order to ensure that the level of protection afforded is "essentially equivalent" to that of the EU. The means to achieve this

was left to the parties. Both the EU and the United States are mutually interested in ensuring that whatever system used for data transfers, adequacy decisions, contracts, binding corporate tools, international agreements, will meet the test of the Court, provided that the continuity of the Union's level of protection is ensured.

However, regarding the Safe Harbour and now the new Privacy Shield the Parliament has consistently expressed its concerns about their legal certainty and whether they are "court proof". We want a system that complies with the Charter and the Union data protection law. The EP resolution of 25 April 2016 confirmed this approach, and called for the implementation of the recommendations of the Union Data Protection Authorities (Article 29 Working Party and the EDPS) to make it a stronger instrument. We made it clear that if this was not the case, the Privacy Shield risks not achieving the goal for which it has been established and could be challenged at the Court.

3. LIBE Committee resolution

The Commission formally adopted the Implementing Act on the adequacy of the Privacy Shield on 12 July. While the final agreement took a number of our concerns into consideration, the LIBE Committee has now decided to work on a further Parliamentary resolution as many of the Parliament's concerns still remain. We do not have the power to veto the agreement, but, as numerous criticisms have been raised, the LIBE Committee has decided to adopt a resolution expressing our concerns.

We want a data transfer system that complies with the Charter and Union data protection law. To do so, the Privacy Shield should respond to the concerns that were highlighted by the Article 29 working party on its compatibility with Union law. These include concerns regarding the principle of data retention, the bulk collection of personal data for national security purposes, the need for sufficient judicial redress and effective independent oversight as well as several law enforcement issues. As I said earlier, if these concerns are not taken into account the Privacy Shield risks not achieving its purpose and could be challenged in the Court.

In our preparation of the LIBE resolution, the LIBE Committee has met with the Commission (DG JUST), and with representatives of the Article 29 Working Party for an exchange of views on the adopted version of the Privacy Shield. This enabled our Committee to hear the improvements that had been made to

the agreement since the Parliament's April 2016 resolution, and to take note of concerns and clarifications still needed with the arrangement.

The Commission stressed that it had taken note of the concerns expressed by the Article 29 Working Party in their opinion of 13 April 2016. The Article 29 Working Party welcomed the additional provisions and safeguards which included additional clarifications on bulk collection of data, strengthening the Ombudsperson mechanism, and more explicit obligations on companies as regards limits on retention and onward transfers, but nevertheless highlighted a number of remaining concerns regarding both the commercial aspects and the access by U.S. public authorities to data transferred from the EU.

The LIBE resolution will be presented in our Committee next week on 12 January, and is expected to be adopted in plenary in March 2017.

4. Concerns that remain with the final agreement

The Parliament could therefore use this opportunity to highlight a number of key concerns in the LIBE resolution. Specifically:

- **The need for independent and effective oversight**: As highlighted in the Schrems case, there is still a need for independent and effective oversight. It is still questionable if the mechanism of the Ombudsperson which has been developed specifically by the US authorities for the Privacy Shield, has sufficient powers to function effectively and if he/she is really independent. According to Article 8 of the Charter, compliance with data protection rules shall be subject to control by an independent authority. This principle was repeatedly confirmed by the jurisprudence of the European Court of Justice.

- **Mass surveillance and wide national security exceptions:** The U.S. administration does not fully exclude the massive and indiscriminate collection of personal data originating from the EU, although the U.S. has another interpretation of what targeted and bulk surveillance mean. Although the ODNI has committed not to conduct mass and indiscriminate collection of personal data, there not been any concrete assurances that such a practice would not take place and, as such, this would not satisfy the standards of the Court. Data protection authorities have also stated that mass surveillance of individuals can never be considered as proportionate and strictly

necessary in a democratic society, as is required under the protection offered by the Charter of fundamental rights.

- **The question of non-citizens' access to judicial redress**: this is still not remedied as there is a lack of clarity as to who can be considered to be an EU individual and would therefore benefit from protection under the Privacy Shield: all EU citizens or all persons residing in the EU. The Judicial Redress Act developed in the framework of the Umbrella agreement would not apply to non-Union citizens either.

- **Questions still remain regarding the relationship between the Privacy Shield and General Data Protection Regulation** when it comes into force in May 2018. The Privacy Shield does not reflect the future requirements of the new data protection regime, such as the additional obligations which will apply to data controllers - like carrying out data protection impact assessments. The joint annual review of the Privacy Shield will therefore be crucial in order to integrate these concerns.

- In addition, we will also emphasise that the Commission followed the procedure for adoption of the Commission implementing decision in a manner that resulted in **depriving the Parliament from properly expressing its right of scrutiny** on the draft implementing act, without respecting the Inter-institutional agreement between the Commission and the Parliament – for instance, Member States were kept informed via the Committee of the Article 31 of the modifications of the text before the Parliament while the Parliament was only informed at the end of the procedure.

5. Scope to improve the agreement - Annual Review

The first joint annual review will be a key moment for the Privacy Shield mechanism to be further assessed, as stated by the Article 29 Working Party. However, this joint annual review will only be successful if several conditions are met. It will be particularly important in the course of the joint review to ensure that the competences of all the members of the joint annual review team, including the Data Protection Authorities, are clearly defined. In addition, all members of the joint review team should have the possibility to directly access all the information necessary for the performance of their review, including elements allowing a proper evaluation of the necessity and proportionality of the collection and access to data transferred by public authorities.

Another important element is that any member of the joint review team should be ensured its independence in the performance of its tasks and should be entitled to express its own views in the final report of the joint review which would be public and annexed to the joint report. This would also allow the Parliament to carry on its scrutiny powers.

When participating in the review, the national representatives of the WP29 have stated that they will not only assess whether the remaining issues have been solved, but also whether the safeguards provided under the EU-U.S. Privacy Shield are workable and effective.

The Parliament will continue to pressure the European Commission to take measures to ensure that the arrangement provides a protection of personal data which meets the requirements of the Charter of Fundamental Rights and the Data Protection legal framework, which will apply from 16 May 2018.

6. Impact of Brexit on data protection matters

Going forward, the European Parliament will continue to scrutinise this process, in addition to the many possible scenarios regarding the impact of Brexit on data protection matters. Whether the UK continues to abide by the new data protection regime post-Brexit is an important question, particularly, as I'm sure you know, because UK companies will not be able to avoid complying with the GDPR completely.

After the UK's withdrawal from the EU, data transfers from the EU to UK will have to comply with data protection rules on third country transfers, unless a specific arrangement is found in the Brexit treaties. A possible arrangement could be to consider the UK providing an adequate level of protection, assuming that it has fully implemented the EU data protection law. This would allow free transfers from the EU to the UK.

However, the adequacy of the UK implies that the EU law on data protection remains unchanged to ensure that UK is "always" adequate. Therefore, if EU law is modified UK national legislation will also need to be modified.

The UK companies and organisations that process personal data of EU citizens will have to continue applying the EU legislation to those data. Moreover, the new Regulation requires organisations, which process EU citizens' personal data and are not established in the EU, to appoint a representative in the respective Member State.

The UK regulator - ICO - has said that data protection standards will have to be equivalent once the UK leaves the EU to ensure consistency for companies and organisations operating across borders. They have therefore called for reform of UK law (to implement EU data protection law) to make sure that this is the case.

There are several possible scenarios regarding the transfer of personal data from the EU to the UK, as the UK would become a "third-country" in terms of EU data protection law. To ensure the flow of data between the two, the following solutions could be envisaged: Standard Contractual Clauses between the UK and EU data controllers and processors; a UK adequacy assessment; or a self-certification scheme such as a UK "Privacy Shield".

The most likely situation would be that the UK adopt something very similar to the GDPR and would then apply to European Commission for adequacy status. This means that the Commission would examine the UK's data protection law and, if it felt that it offered equivalent protection to the personal data as the GDPR, then it would allow the UK to receive personal data from the EU without the need for other data transfer mechanisms. A number of countries, including Canada, New Zealand, Argentina and Israel, have gone have undergone this process.