White Paper

Transatlantic crossings: the Future of EU-US Data Flows

March 2021

Authors:

Think NEXUS Policy Expert Group

Think NEXUS, an EC-funded project, aims at reinforcing EU-US collaboration on NGI-related topics in three focus areas: Science and Technology, Innovation and Entrepreneurship and Policy. The aim is to boost strategic research, industrial partnerships and policy compliances in order to gain socio-economic benefits in both the EU and US regions.

In the framework of this project, we are regularly publishing several short articles aiming at comparing the US and the EU approaches in different topics of NGI. The present document is focusing on Artificial Intelligence.

THI
NK
NEX
US

Introduction

In the past 30 years, there has been an important globalisation of ICT infrastructures. Therefore, data flows and free flows of data have become more and more important for the European and the US economy and with it comes the importance to be able to exchange data between these two regions in a simple manner.

Nevertheless, the data protection legislations in Europe and in the US are different. In order to facilitate and to enable a simple data exchange between the two transatlantic regions, they need to build equivalent data protection laws.

Between 1998 and 2000, the Safe Harbour Agreement was elaborated and signed. This set of principles aimed at ensuring the data transfers between the EU and the US complied with the European Data Directive 1995. It was based on the following 7 principles[1] :

- **Notice:** Individuals should be informed that their data has been collected, how it will be used and how to contact the data holder for any queries;
- **Choices:** Individuals should be able to opt out as well as forward the relevant data to another third party;
- **Onward Transfer:** the transfer of any data can only happen with a third party that meets the required data protection principles;
- **Security:** a reasonable effort must be made to keep the data safe from loss or theft;
- **Data Integrity:** the data must be relevant and reliable for its original purpose of collection;
- **Access:** individuals should be able to access, correct and delete any information held about them;
- **Enforcement:** there must be effective means of enforcing these rules.

The Safe Harbour Agreement was based on a self-certification mechanism: each US companies self-certified that it will respect the data protection requirements from the EU. But some doubts regarding the effectiveness of this mechanism emerged and a legal case against this agreement was started and led by Max Schrems.

Therefore, the Safe Harbour Agreement was declared invalid by the European Court of Justice (ECJ) in October 2015. This led to further discussions between the EU and the US around “a renewed and sound framework for transatlantic data flows with a higher level of protection”[2].

1 European Court of Justice 200/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles.

2 https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_15_5916

The EU-US Privacy Shield and its invalidation

Result of these discussions was the adequacy decision on the EU-US Privacy Shield adopted on the 12th of July 2016 (Decision 2016/1250) which became operational on the 1st of August 2016. This new arrangement aimed at providing stronger obligations on companies in the US to protect the personal data of Europeans and at stronger monitoring and enforcement by the US Department of Commerce and Federal Trade Commission (FTC), including through increased cooperation with European Data Protection Authorities[3] .

"The new EU-US Privacy Shield will protect the fundamental rights of Europeans when their personal data is transferred to US companies. For the first time ever, the US has given the EU binding assurances that the access of public authorities for national security purposes will be subject to clear limitations, safeguards and oversight mechanisms. Also, for the first time, EU citizens will benefit from redress mechanisms in this area. In the context of the negotiations for this agreement, the US has assured that it does not conduct mass or indiscriminate surveillance of European." Commissioner Jourová[4]

The Privacy Shield arrangement included the following elements:

- Strong obligations on companies handling Europeans' personal data and robust enforcement;
- Clear safeguard and transparency obligations on US government access;
- Effective protection of EU citizens' rights with several redress possibilities.

However, this regime was also attacked in ECJ arguing that it still not is sufficient to guarantee the security of personal data. And indeed, on the 16th of July 2020, the ECJ issued a judgment declaring as invalid the Safe Harbour Agreement.

Therefore, this facilitated framework for data transfers has been abolished and the US was put on the same level than other countries which does not have a positive adequacy, meaning that companies could still use data transfer mechanisms that were available for other countries such as standard contractual closes and other corporate mechanisms.

3 https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216
4 https://ec.europa.eu/commission/presscorner/detail/en/IP_16_216

Consequences of the invalidation of the Privacy Shield and the new challenges

In practices, the invalidation of the Privacy Shield is inconvenient for many companies as using standard contractual clauses implies heavy administrative overhead. Indeed, it requires companies to conduct an assessment of themselves to guarantee that their particular circumstances taking into account all the details of their data processing activities, the scope, the scale of the data and its sensitivity, the likelihood that could be targeted, etc. are adequate to protect personal data. This is currently a heavy burden for many companies and this legally complicated situation is not going to get solved until the US and the EU agree on a political arrangement that streamlines the relationship again between the EU and the US as the Safe Harbour Agreement and the Privacy Shield Agreement did. This is particularly true as more than 5 300 companies in the US relied on the Safe Harbour Agreement and most of them are small and medium-sized companies which are scrambling to find a basis under EU law for transferring personal data.

For the US, this invalidation of the Privacy Shield Agreement is much larger than just a privacy issue: it is a national security issue which is an important challenge. Indeed, this invalidation raised questions regarding the standard contractual clauses, created new obligations on data exporters and imposed certain obligations on data protection authorities. These findings have created uncertainty regarding transatlantic data flows specifically as well as data transfers from the EU to certain other countries more broadly. The gist of this invalidation is: the subject seems to be a transatlantic matter, but the implications are much broader.

In addition, since the invalidation of the Privacy Shield, the US Commerce Department and the European Commission have published press releases and have committed to try to work together to build a framework addressing the core fundamental rights expressed by the ECJ in its decision. The ECJ observed that the US surveillance program conducted under the Section 702, the US Foreign Intelligence Service Act or the Executive order 12-333 both do not grant surveilled persons actionable of redress before independent and import in impartial court. The ECJ also identified two ways in which US surveillance law lacks essential equivalence to EU legislation: EU safeguards and more specifically the lack of an effective and enforceable right of individual redress and the issue of proportionality.

Moreover, another challenge is that with the ECJ's invalidation of the Privacy Shield, it is the second invalidation of data protection EU-US agreements and this has created a broader uncertainty of data protection legislation and therefore, of the future of data flows. As a consequence, it can be observed that there is a crisis in the belief of the globalisation of data flows and a resurgence of the importance of data sovereignty. Indeed, more and more countries not just within the EU but also outside the EU have become convinced that their data is such a strategic important asset that they cannot run the risk anymore of foreign authorities, foreign countries exercising control over these data.

Several examples illustrates this trend towards dividing data back into silos: discussions in the US around the social media TikTok that has been required to be sold to a US company in order to keep the data from US citizens in the US and similarly the European Commission is examining possibilities to do the same for Facebook, requiring Facebook to sell its European activities to a European company in order to shield the data. This trend can become a challenge for future EU-US collaboration in data protection as it goes against the work done since the last 20 to 30 years in this domain.

Next steps and recommendations

On the European side, companies that used to rely on the Privacy Shield Agreement now have to rely on another mechanism, the standard contractual clauses if they want to continue to transfer data to the US. Therefore, they have to identify whether there are adequate safeguards for the transfer of personal data and to screen what the risks are for the data to be intercepted and what can be done to mitigate those risks. Moreover, this assessment needs to be done on a case-by-case basis. The existing fundamental conflicts are between the safeguards that EU data protection laws expect to have versus the competences that apply in other countries. Therefore, for most research projects or organisations, the short term solution consists in assessing which kind of data transfer activities they are engaged in, assessing which risks are to run for those data processing activities and identifying whether they have alternatives that are easily available either through technical measures to mitigate the risk by scaling down the amount of data being transferred, or by looking for alternative providers. Nevertheless, none of these options are particularly viable, none of them are sustainable and all of them seem to be harmful in terms of societal progress. But, on the short term and on the scale of an individual research organisation, these solutions seem to be the only practical resources available. Other potential solutions are much more complicated and part of a much larger picture that cannot be influenced by companies or research projects.

In order to build a new EU-US collaboration framework regarding data flows, both sides of the Atlantic are undergoing specific actions.

Indeed, in the EU, discussions on the importance of standard contractual clauses have been engaged. Moreover, in early September 2020, the European Data Protection Board has formed two different task forces aiming at revising and updating standard contractual clauses. This will be important to enhance the trust and confidence between the US and the EU. In addition, the European Commission and more specifically the DG Justice are working on revising standard contractual clauses.

In the US, the US Department of commerce has issued a white paper[5] specific on the issue of transferring data between the EU and the US. It explains that a case by case analysis needs to be undertaken but that part of the analysis concerns the nature of the data being transferred. Indeed, if the transferred data is not likely to be part of a national security letter request or under surveillance law in the US, the process for transferring data becomes much easier. On the other hand, if it is likely to be part of a national security letter request or under surveillance law in the US, the process is more time consuming. Through this white paper, the recommendation guidelines on the additional measures and safeguards through the standard contractual clauses have been extensively formalised and organisations can related to this white paper to learn about what needs to be done to transfer data from the EU to the US. One of the recommendations of this paper would be for the European Data Protection Board to produce a similar paper on its own expectations so companies could merge those and decide if they are able to work under those current terms, this existing legislation and these existing policies.

Even if the standard contractual clauses and other mechanisms as anonymisation and encryption techniques seem to be a solution to the privacy issues related to the transfer of data between the EU and the US, there is a crucial need for a US Federal privacy law and the perspective of building such a law seems to be very optimistic since more progress has been made to this regards in the last 2 years than in the last 20 years. The US is not going to solve the national security implications of the invalidation of the Privacy Shield, but it will get them closer to a value of privacy in a broader term. Indeed, current discussions in the US concern a higher baseline for privacy and data. Now, these discussions are also impacted by the new US President election which has been resulting in a new administration. Data privacy is still a high priority but as the administration is newly formed, the discussions and activities to this regard will probably take more time which does not enable to provide a specific timeline for a new agreement succeeding the Privacy Shield.

5 https://www.commerce.gov/sites/default/files/2020-09/SCCsWhitePaperFORMATTEDFINAL508COMPLIANT.PDF

NGI THINK NEXUS

thinknexus.ngi.eu @ThinkNEXUS_NGI

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825189. This publication reflects only the author's view and the Commission is not responsible for any use that may be made of the information it contains