What's Wrong with the Privacy Shield?

The New Privacy Shield

On the 6th October 2015, the European Court of Justice (the 'ECJ'), in *Maximilian Schrems vs Data Protection Commissioner*,[1] decided that the Safe Harbor Agreement[2], a set of privacy and data protection principles made by the United States and later confirmed by the European Commission, and which governed the relationship of US' businesses and entities with EU based data, which had been in force since 2000 was no longer adequate to counter the advancements in privacy and data protection, which included the consequences of the Snowden revelations. The United States' public authorities regularly carried out secretive mass surveillance operations and this, together with huge amounts of personal data relating to millions of individuals connected to social media, were the major elements that brought about this decision which set the data protection field into a frenzy. The Court, in fact, found that social media sites and other digital operators do not provide customers with protection from state surveillance. While the decision itself was not a complete surprise, considering the Safe Harbor Agreement was 15 years old and thus did not cater for the humungous technological advancements made, experts had opined that such a decision would not be so forthcoming in the immediate but changes would take place gradually with the Commission at the helm. Yet, it was. Indeed, EU citizens and especially commercial entities in the US or holding data centres in the US, entered into a limbo wherein the Safe Harbor Agreement could no longer provide a basis for transfers of data to the US.

The above-mentioned decision meant that the EU and the US needed to negotiate a new agreement which addressed the inadequacies raised by the ECJ – and had to finalise it quickly. In February 2016, the draft adequacy decision known as the Privacy Shield[3] was published by the European Commission. This Privacy Shield provided for further obligations for companies in the US in order to protect the personal data of EU individuals and further cooperation between the US authorities and their EU counterparts including data protection departments across the EU. This included written commitments from the US authorities stating that bulk collection of data transferred from the EU to the US should only occur under specific, and proportionate, conditions, and that indiscriminate mass surveillance of the data transferred should be prohibited while access to such data given to US public authorities should be limited and safeguarded. The Privacy Shield was welcomed by businesses, entities and public authorities alike. However, it was immediately recognised that this was not as revolutionary as it may have seemed at first glance.

Both the Article 29 Data Protection Working Party (the 'Working Party') and the European Data Protection Supervisor (the 'Supervisor') issued opinions on how the Privacy Shield would need to be improved in order to safeguard important European principles.

Fundamental Principles remain Unprotected

On 13th April 2016, the Working Party issued *Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision.*[4] Following this, on the 30th May 2016, the European Data Protection Supervisor, Mr Giovanni Buttarelli also issued his *Opinion on the EU-U.S. Privacy Shield draft adequacy decision*.[5] The Supervisor welcomed the improvements made to this new agreement in relation to the previous

[1] http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=en

[2] Commission Decision 2000/520/EC, of July 26, 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protect Provided by the Safe Harbor Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000

[3] http://ec.europa.eu/justice/newsroom/data-protection/news/160229_en.htm

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf

[5] https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf

Safe Harbor Agreement. However, he stated that *"progress compared to the earlier Safe Harbor Decision is not in itself sufficient. The correct benchmark is not a previously invalidated decision, since the adequacy decision is to be based on the current EU legal framework."*[6] The Working Party pointed out that the Privacy Shield needed to be consistent with all EU data protection regulations including the new Regulation (EU) 2016/679 (known as the 'General Data Protection Regulation'), which was yet to enter into force. Therefore, a review of the Privacy Shield within this context, in the future, was necessary according to the Working Party. This was also reiterated by the Supervisor.

The Working Party insisted that the Privacy Shield should ensure an essentially equivalent level of protection to that under EU legislation. Therefore, fundamental principles had to be clearly laid out. The Working Party mentioned the lack of a clear data retention principle, the lack of a prohibition of strictly automated processing decisions, and the lack of clear limitations to the purpose principle. The Supervisor also mentioned that provisions in relation to the right to access and right to object were to be better clarified. Importantly, the Supervisor noted that the rights of access, rectification or erasure concerning individuals' personal data were not fully addressed in the then-current draft of the Privacy Shield. The Privacy Shield stated that its basic principles may be limited to the extent necessary to meet national security, law enforcement or any public interest requirement. It further created limitations to the principles in case of regulation or case law creating conflicting obligations or explicit authorisations. This brought about questions of interpretation as to the limitations at play. The Supervisor advised that in all such cases, *"the purposes for which exceptions are allowed and the requirement of a legal basis should be more precise".*[7] Otherwise, the limitations included would be a repeat of the limitations in the Safe Harbor Agreement which were deemed invalid since there was no clarification on such interferences by US authorities with regard to the rights of the persons whose data is transferred from the EU. It seemed that the Supervisor's major point of recommendation was for the EU to hold more supervision and monitoring and be able to enforce the fundamental principles of data protection in the US, notwithstanding the exemptions and exceptions integrated into the Privacy Shield.

The Supervisor raised a particular point regarding journalistic material and stated that there was an obligation to balance the right of freedom of expression with the rights of privacy and data protection as a fundamental principle of law, and therefore, a general exemption relating to such processing should be changed into specific derogations, when needed. After all, this was a significant point in the Court's decision which rendered the original Safe Harbor Agreement invalid.

The Supervisor also recommended that the Ombudsman established pursuant to the Privacy Shield should be able to act independently from any authority and required further serious commitments from the US that any requests, decisions and recommendations given by the Ombudsman would be effectively respected and implemented by the bodies concerned. The concern here was that without clear provisions entailing such effective implementation, the Ombudsman would become a mere figurehead. The Working Party also insisted that the remedies included for EU citizens were as unclear and complex as to possibly prove ineffective and unusable.

The Way Forward

Vital aspects such as fundamental principles and redress were tackled by both authorities' reports and surely, such elements needed to be taken into consideration by the Commission.

The EU-US Privacy Shield, however, was officially ratified on the 12th July 2016. It entered into force in the EU on the same date. It seems that commercial interests of both the EU and the US made the

[6] Ibid. Page 6.
[7] Ibid. Page 7-8

process of finalisation quicker and not much time for assessment was allowed. This final Privacy Shield, as approved, had been further revised. The fundamental purpose limitation principle was further clarified and now states that business entities may not process the personal data in a way that is incompatible with the purpose for which that data was collected initially. In fact, the data may only be retained as long as the purpose for which it was collected subsists. This is further in line with EU data protection legislation. The final Privacy Shield was also amended with regard to transfers of EU personal data to third countries in that it was sought to protect EU personal data from being indiscriminately processed without regulation once outside the direct scope of the Privacy Shield. The Commission has also potentially increased the responsibility of national data protection authorities, following the advice of the Working Party and the Supervisor. In fact, such national authorities may have a role in pursuing breaches and complaints. However, this role is very limited and is only highlighted as a potential use. The national authorities, for example, have the power to oversee processing of data if the entity has voluntarily submitted itself to such oversight. This brings about doubts as to how convenient and practical it shall be and if it will be used at all and to which extent.

Other aspects also still remain in doubt. The position of the Ombudsman is not sufficiently clarified and in any case the Ombudsman only deals with enforcement regarding public intelligence authorities. Additionally, its independence and effective redress capability are still questionable. Furthermore, the Privacy Shield still does not furnish EU citizens with protection or even readily available redress mechanisms against the Ombudsman's decisions on automated processing.

Therefore, although a lot of advancements have been made in order to make the Privacy Shield better and in accordance with the updated EU fundamental data protection principles, the result is not completely satisfactory. Issues of automated processing and indiscriminate surveillance and access by US public authorities still remain unclear and further public knowledge of data protection violations may interfere with such efforts being made by the EU and the US authorities. While US companies started collecting and processing data under the Privacy Shield as from 1st August 2016, all parties must remain vigilant as risks are still inherent to the Privacy Shield itself, the elements of protection it covers and their extent. It is clear that European authorities have no intentions of quieting down. The French *Commission Nationale de l'Informatique et des Libertés,* for example, issued a decision on the 20th July 2016 wherein it ordered Microsoft to stop collecting excessive data from its EU citizen users, such as tracking the browsing of users for marketing and advertising purposes without the users' consent, within a three-month timeframe. This kind of decision is not a one-off and several US companies have had their procedures analysed and criticised for data protection violations against EU citizens, by judges, authorities and watch dogs alike. It remains to be seen how this will continue following the Privacy Shield's entry into force.

The users' adherence to the data protection principles under the Privacy Shield will have to be assessed in the future years. It must be noted that such entities might consider abiding by general EU data protection concepts and principles in the event of lack of clarity of same in the Privacy Shield. EU authorities' will continue their monitoring, and nothing excludes the ECJ from issuing another decision which might disavow the Privacy Shield in the future. It has been strongly suggested, after all, that certain aspects of the Privacy Shield remain dubious.