LOCKE LORD® QUICK Study
Privacy & Cybersecurity Practice
February 3, 2016

New Safe Harbor Agreement For EU Data Transfer Announced

By: Mark E. Schreiber, Alan D. Meneghetti, Thomas J. Smedinghoff and Natasha Ahmed

Companies are relieved that there will now be a new Safe Harbor for cross-border transfer of personal data from Europe to the US.

This announcement will provide a degree of certainty going forward, in particular after the upheaval which the *Schrems* case decision of the European Court of Justice last year produced, striking down the then existing Safe Harbor framework. Businesses should, however, also expect a more rigorous process by the US Department of Commerce to qualify for the "new" Safe Harbor certification and by the FTC to enforce it.

Both the EU authorities and the FTC issued statements on 2 February announcing the agreement highlights.

While it will take some time for the authorities to reduce these elements to detailed text and obtain formal approval, several new components of the Safe Harbor arrangements (now referred to as the EU-US Privacy Shield) are already clear from the announcements:

Strong obligations on companies handling Europeans' personal data and robust enforcement.
U.S. companies wishing to import personal data from Europe will need to expressly commit to robust obligations on how personal data is processed and individual rights are guaranteed. The Department of Commerce will monitor companies' published Safe Harbor commitments for enforcement by the FTC. In addition, any company handling human resources data from Europe has to commit to comply with decisions by the various European Data Protection Authorities (DPAs).

Clear safeguards and transparency obligations on U.S. government access.
The US has given the EU written assurances that access by US authorities for law enforcement and national security will be subject to clear limitations, safeguards and oversight mechanisms. The US has also, significantly, ruled out indiscriminate mass surveillance on personal data transferred to the US under the new arrangement. To regularly monitor the arrangement there will be an annual joint review, which will also include the issue of national security access. The European Commission and the US Department of Commerce will conduct the review and invite national intelligence experts from the US and European DPAs to it.

Effective protection of EU citizens' rights with several redress possibilities.
Any EU citizen who considers that their data has been misused under the new arrangement will have several redress possibilities. Companies will have deadlines to reply to complaints, and European DPAs can refer complaints to the Department of Commerce and the FTC. In addition, an Alternative Dispute Resolution process to address complaints will be provided free of charge, giving real teeth to the right of redress, something which was a major concern to the EU authorities during the course of the negotiations. For complaints on possible access by national intelligence authorities, a new Ombudsperson will be created.

Of course, we will need to see what the final text of the Safe Harbor framework looks like and, ultimately, what the regulations and guidance to be issued by the Department of Commerce and FTC around this will require. In addition and, as is so often the case, the practical implementation of the framework will be crucial.

In the meantime and until the text of the new Safe Harbor framework is agreed and published, businesses can continue to rely on model clauses, consents obtained from data subjects from whom data is collected and binding corporate rules. However, the EU Article 29 Working Party (a policy body made up of EU DPA heads) has also indicated in very recent announcements that they have concerns regarding the appropriateness of model clauses and binding corporate rules for transfers to the U.S., and will be reassessing those mechanisms in light of the new Privacy

Shield framework once it is released. Thus, while they made clear that business may rely on model clauses and binding corporate rules in the interim, that issue will be subject to review expected to be completed by the end of April. Thus, as we indicated earlier, businesses should reevaluate their current EU data collection processes and consider other steps. The new EU GDPR due to be finalized this spring may have some effect on this also.

Here are some suggested steps for the near term:

- Identify personal data flows of the company from the EU to U.S., including employee, customer and lead data. Identify the path that the personal data follows, from its collection by the EU company, to its transfer to the entity in the U.S., and any onward transfers; identify the purposes for which the personal data is collected and used; and identify the systems, software and hardware used by or on behalf of the company to store and process the personal data. Determine which EU countries the data is being transferred from, as the oversight and positions of EU national DPAs may be different.
- Identify all instances of where the company relies (or relied) on Safe Harbor (or on other cross-border data transfer mechanisms), including, for example, in intra-group transfers, and transfers to US vendors, partners, sub-processors, and sub-contractors. Review the data protection due diligence on these EU and US entities.
- Check if other derogations or exclusions apply, such as consent or transfers that are necessary for the performance of a contract with the individual in respect to whom the personal data relates, or for compliance with a legal obligation. If the company relies on consent, ensure that the company's privacy policies, notices and consents are adequate and effective (do they explicitly allow transfers of the personal data to the US), and that the company does not process (at least going forward) the personal data of anyone who has withdrawn their consent.
- Review the company's public or consumer-facing statements (such as terms and conditions, promotional content, current contracts with customers) and make sure that nothing misstates the data protections or privacy practices which the company has in place. This may need to include disclaimers as to current Safe Harbor invalidity in the company's posted Safe Harbor privacy policy, according to the FTC.
- Review indemnity provisions in the company's agreements with relevant service providers, third parties and other entities in the data processing and transfer chain so as to ensure that any privacy related risks are addressed.
- Identify the implementation mechanisms, means and back-off steps whereby Safe Harbor, EC Model Contract Clauses, and/or consents are actually put into effect or accomplished.
- Identify relevant stakeholders in the process and inform them, where appropriate, of their obligations. These may include company or third party sales representatives, distributors, data gathering entities, customers, and other employees.
- Consider the impact on current and upcoming projects of the company, including technology resets or re-configurations.
- Review your exit, break, force majeure and compensation clauses in existing contracts that may have exposure, and initiate strategic discussions regarding privacy and data protection amendments to these contracts.

Mark E. Schreiber | 617-239-0585 | mark.schreiber@lockelord.com
Alan D. Meneghetti | +44(0) 20 7861 9024 | ameneghetti@lockelord.com
Thomas J. Smedinghoff | 312-201-2021 | tom.smedinghoff@lockelord.com
Natasha Ahmed |+44(0) 20 7861 9024 | nahmed@lockelord.com