KING & SPALDING

Client Alert

Business Litigation Practice Group
Data, Privacy & Security Practice Group

For more information, contact:

Phyllis B. Sumner
+1 404 572 4799
psumner@kslaw.com

Jane E. Player
+44 20 7551 2130
jplayer@kslaw.com

Angela Hayes
+44 20 7551 2145
ahayes@kslaw.com

Kim Roberts
+44 20 7551 2133
kroberts@kslaw.com

Nicholas A. Oldham
+1 202 626 3740
noldham@kslaw.com

Sebastian D. Müller
+49 69 257 811 201
smueller@kslaw.com

King & Spalding
London
125 Old Broad Street
London, EC2N 1AR
Tel: +44 20 7551 7500

Washington DC
1700 Pennsylvania Avenue, NW
Suite 200
Washington, DC 20006-4707
Tel:+1 202 737 0500

Atlanta
1180 Peachtree Street, NE
Atlanta, Georgia 30309-3521
Tel: +1 404 572 4600

Frankfurt
TaunusTurm
Taunustor 1
60310 Frankfurt am Main
Germany
Tel: +49 (69) 257 811 000

www.kslaw.com

December 20, 2016

EU-U.S. Privacy Shield: Assessing The New Regime

Businesses have now had four months to get to grips with the new EU-U.S. Privacy Shield for transatlantic data transfers after it came into force in August 2016. As the New Year looms, what are the emerging trends we have seen from the new regime?

Background

In March 2016, we reported that the EC and the U.S. Department of Commerce ("Commerce") reached an agreement-in-principle for the new Privacy Shield to improve the protection of personal data and strengthen enforcement mechanisms. Access to that alert is available here.

Following the initial agreement with Commerce the European Commission (EC) approved the Privacy Shield for transatlantic data transfers on July 12, 2016 – replacing the previous Safe Harbor Framework in the process. Our briefing of October 7, 2015 gives further detail about the European Court of Justice's decision to invalidate the Safe Harbor Framework. Access to that alert is available here.

The Privacy Shield improves the protection of personal data and strengthens enforcement mechanisms. It is designed to protect the rights of individuals in the EU whose personal data is transferred to the U.S., as well as bring legal clarity for businesses relying on transatlantic data transfers.

Companies who have certified under the Privacy Shield and those who wish to do so commit to adhere to the following seven principles:

1. **Notice**: Publishing privacy policies and links to Privacy Shield related information;

2. **Choice**: Providing appropriate consent and opt-out mechanisms to users;

3. **Accountability for onward transfer**: Concluding data transfer agreements with third party recipients;

4. **Security**: Implementing appropriate security measures;

5. **Data integrity and purpose limitation**: Ensuring that data is only processed for the purposes for which it has been collected;

6. **Access**: Providing mechanisms to enable data subjects to confirm what processing is taking place, and to correct or delete information held about them; and

7. **Recourse, enforcement and liability**: Implementing mechanisms to resolve complaints.

The new regime was approved in July, with organizations registering from August. During the finalization of the new regime, the EC revised the wording of the Privacy Shield and renegotiated a number of aspects with the U.S., leading to an amended Privacy Shield agreement, containing the following enhanced safeguards:

- ***Stricter rules for processing***: The most important change for businesses that seek to self-certify under the Privacy Shield is that stricter rules have been put in place on several processing activities;

- ***More explicit retention periods***: The existing limitation of data retention has been made more explicit. Companies may keep personal data only as long as this serves the purpose for which the data was collected;

- ***Limitations to secondary processing***: In line with the GDPR, the Privacy Shield provides for a stricter purpose limitation requiring organizations "not to process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual;"

- ***Tightened conditions for onward transfers of personal data***: The obligation to provide the "same level of protection" when passing on data to third party recipients has been further clarified and now includes an obligation for the third party in question to inform the Privacy Shield company when it is no longer able to ensure the appropriate level of data protection. At that point, the Privacy Shield certified company will then have to take appropriate measures, such as making sure that the third party ceases processing;

- ***Limitations around bulk data collection***: An important change that does not so much affect the companies who register with for the Privacy Shield, but which was a precondition for the EU's acceptance of the Privacy Shield as a whole, concerns the bulk collection of intelligence information by U.S. national security administration. It has been specified that data collection by the intelligence services should, as a rule, be targeted. Additionally, the exceptional use of bulk collection of data is limited to six defined national security purposes;

- ***Independence of the Ombudsman***: Redress in the area of national security for anyone whose data is transferred to the U.S. will be handled by an Ombudsman that is independent from the U.S. intelligence services. During the adoption process, the functioning and the independence of the Ombudsman have been further clarified, in particular its independence and its cooperation with other independent oversight bodies with investigatory powers.

Questions so far

At the time of writing over 1130 corporates have signed up to the Privacy Shield. Since registration was approved important questions have emerged, including:

Have all of the concerns about the Privacy Shield been resolved?

The short answer is: no. The Article 29 Working Party published a statement in late July 2016 which welcomed the improvements of the revised Privacy Shield, but said that concerns around the lack of specific rules on automated decisions, the general right to object, and how the Privacy Shield principles apply to processors, had not been fully addressed. It also stated that it would have expected stricter guarantees concerning the independence and powers of the Ombudsman mechanism and that it regrets the lack of concrete assurances that mass and indiscriminate collection of personal data does not take place.

Will the Privacy Shield be subject to a legal challenge?

The consensus opinion from Data Protection Authorities, lawyers and commentators is that the Privacy Shield almost certainly will be challenged before the courts in the not too distant future.

The Article 29 Working Party has said that the first joint annual review will be "*a key moment for the robustness and efficiency of the Privacy Shield to be further assessed*." It has further stated that it will be considering whether the remaining issues have been resolved, but also "*if the safeguards provided under the Privacy Shield are workable and effective.*"

To register or not to register = what should businesses do now?

US organizations have been able to register with US Department of Commerce for the Privacy Shield from 1 August 2016 via a system of self-certification. Our recommendations are:

- For all US companies that have previously relied on Safe Harbor, it is time to decide whether to subscribe to the Privacy Shield. While those companies that have switched to the use of EU Standard Contractual Clauses (SCC, or 'Model Clauses') are not under immediate pressure, those who have waited for the Privacy Shield and not yet implemented an alternative will need to take action.

- U.S.-based companies that receive personal data from EU businesses will have to carefully review the Privacy Shield, as well as their data processing activities, before deciding whether to self-certify under the Privacy Shield. However, bear in mind that not all companies are eligible to register. The privacy principles will apply immediately upon certification and the application process for the Privacy Shield is rigorous.

- With this in mind, it is advisable for those thinking of certifying to thoroughly review their privacy practices and policies and to make sure they are compliant with the Privacy Shield prior to making any final decision about whether to apply, as this will involve a significant commitment of time and resources. Commerce is committed to strict supervision and will verify that companies are registered with their designated independent recourse mechanisms prior to finalizing a company's certification. Once a company is party to the Privacy Shield, Commerce can require compliance in the event a failing or remove the company from the list if failings are persistent.

- The GDPR, which comes into effect in May 2018, will bring about even stricter obligations than those under the Privacy Shield. Within two years, U.S. businesses that will be directly subject to the GDPR will have to comply with those enhanced obligations. Many of our clients have taken the view that it is sensible to sign up to the Privacy Shield first, thereby taking a step-by-step approach to bringing their processing operations in line with GDPR requirements.

- Doubts have been expressed as to the legality of the new Privacy Shield, and it is very likely that it will be tested in EU courts sooner rather than later and could be invalidated as a result. Furthermore, at the time of the annual review by the Article 29 Working Party, it is very likely to be subject to further scrutiny and/or amendment. We therefore advise that you put (or keep) in place SCCs as another layer of protection, at least for a certain period of time whilst the position is clarified.

- The Privacy Shield does not affect the validity of SCCs, which remain a valid ground for transferring data outside the EU. Therefore, there is no need to use the Privacy Shield to cover any data transfers made under those SCCs. Yet, since the SCCs' validity is already being challenged before the High Court in Ireland, with a possible referral to the European Court of Justice, companies may have to resort to the Privacy Shield sooner than expected in case SCC-based U.S. data transfers suffer the same fate as Safe Harbor.

More changes in the EU data privacy space

Final approval of the Privacy Shield comes amidst a series of substantial changes to European data privacy laws including:

- The implementation of the General Data Protection Regulation ("GDPR") which will replace existing EU data privacy laws in May 2018. The GDPR aims to strengthen data protection in the EU in a variety of ways, including tightening the rules around consent, requiring corporate regulation of data protection matters and significantly increasing the penalties for violations of the law; and

- The first EU Directive on Cybersecurity, which must be implemented by EU member states by May 2018. This aims to improve cybersecurity capabilities, increase cybersecurity cooperation within the EU, and impose risk management and reporting obligations on "operators of essential services" and digital service providers.

King & Spalding's Data, Privacy & Security Practice

With more than 60 Data, Privacy & Security lawyers in offices across the United States, Europe, and the Middle East, King & Spalding is able to provide substantive expertise and collaborative support to clients across a wide spectrum of industries and jurisdictions facing privacy and cybersecurity-based legal concerns. We apply a multidisciplinary approach to such issues, bringing together attorneys with backgrounds in corporate governance and transactions, healthcare, intellectual property rights, complex civil litigation, e-discovery, government investigations, government advocacy, insurance recovery, and public policy. Our Data, Privacy & Security Practice has unparalleled experience in areas ranging from providing regulatory compliance advice, to responding to security incidents including data breaches and cybersecurity incidents, interfacing with stakeholders and the government, engaging in complex civil litigation (such as class actions), handling state and federal government investigations and enforcement actions, and advocating on behalf of our clients before the highest levels of state and federal government.

* * *