DrinkerBiddle

The EU-US Privacy Shield

March 9, 2016

Welcome

- Overview
  - How Did We Get Here? *Schrems* and Its Aftermath
  - What Happens Next? Article 29 Working Party Opinion
- The Draft Privacy Shield Text
  - Comparison to the Safe Harbor
  - New Rules for Transfers to Third Parties
  - Privacy Shield vs. Model Clauses
- FTC Enforcement
  - Changes to Notice Requirements
  - New “Posting” Obligations
- Q&A

DrinkerBiddle

Today's Speakers

Peter Blenkinsop
Peter.Blenkinsop@dbr.com

Stan Crosley
Stanley.Crosley@dbr.com

Katherine Armstrong
Katherine.Armstrong@dbr.com

Reed Abrahamson
Reed.Abrahamson@dbr.com
Moderator

DrinkerBiddle

Overview

How Did We Get Here? What's Next?

Overview – How Did We Get Here?

- Since 2014 – Department of Commerce and EU Commission have conducted negotiations to revise the Safe Harbor
- October 6, 2015 – Court of Justice of the European Union issues ruling in *Schrems v. Data Commissioner*, invalidating EU-US Safe Harbor
- Article 29 Working Party announces it will begin coordinated enforcement actions in February 2016 if no progress with EU-US negotiations
- February 2, 2016 – Agreement on Privacy Shield announced
- February 29, 2016 – Text of Privacy Shield released

Overview - What Happens Next?

- Article 29 Working Party will be meeting on April 12 and 13 to review the text and will provide an advisory opinion to the EU Commission.
- Following that, the EU Commission will need to issue a formal "adequacy decision."
- Early May seems like the earliest the Privacy Shield could be operational.
- *But . . .* New EU General Data Protection Regulation will likely pass in near future and be effective in 2018. GDPR has requirements that go beyond those contained in the Privacy Shield.

DrinkerBiddle

The Draft Privacy Shield Text

Text of Privacy Shield Released

- Text of Privacy Shield, along with draft adequacy decision from EU Commission, released on February 29.
- Article 29 Working Party will be meeting on April 12 and 13 to review the text and will provide an advisory opinion to the EU Commission.
- Following that, the EU Commission will need to prepare and issue a formal “adequacy decision”
- European Parliament intends to hold hearings on the new framework, but Parliament has no role in approval
- Privacy Shield could be operational sometime before end of June, if no opposition raised by Art. 29 Working Party or EU member states.

What is in the Privacy Shield?

- Very similar to previous EU-US Safe Harbor.
  - In many cases, the text of the Principles and FAQs has been retained with only minor revisions.
  - Many wonder what the reaction of the Article 29 Working Party will be to this approach, which does not appear to address many of the points raised in the Article 29 Working Party's 2014 criticism of the Safe Harbor.
- Privacy Shield is still based on a "self-certification" regime. Company's wishing to take advantage of the Privacy Shield would complete paperwork with the Department of Commerce and subject themselves to enforcement actions brought by the FTC.

Key Changes: New Enforcement Mechanisms

- Privacy Shield certified companies must respond promptly to inquires from the Department of Commerce.
  - European data protection authorities can submit complaints to the Department of Commerce, who will then follow-up with companies.
- Independent recourse mechanisms must be free to individual data subjects.
- New arbitration provisions that can be invoked by a data subject to seek equitable relief upon delivery of appropriate notice.
  - Only for “residual claims” that have not been “resolved by any of the other Privacy Shield mechanisms”
  - Arbitrators will be selected from list created by US Dept. of Commerce and European Commission.
  - Arbitration procedures are “to be determined” but will be “an existing, well-established set of U.S. arbitral procedures (such as AAA or JAMS)”
- Any FTC or court order showing non-compliance must be made public by the company.

Key Changes: More Detailed Notice Requirements

- Link to Privacy Shield list
- Include list of entities or subsidiaries also covered by Privacy Shield
- State commitment to Privacy Shield for all personal information received from the EU under the Privacy Shield
- Describe right of access to personal data
- Identify the independent dispute resolution body and identify it as either a panel of DPAs, an ADR provider in the EU, or an ADR provider in the US
- State which US enforcement agency has authority over the company
- Describe availability of arbitration
- Explain when required disclosures to law enforcement or national security agencies might be made
- Describe liability when transferring data to third parties

Key Changes: Onward Transfers to 3rd Parties

- Privacy Shield requires contracts with third-parties who receive covered personal information: “Organizations must also enter into a contract with the third-party controller that provides that such data may only be processed for limited and specified purposes consistent with the consent provided by the individual and that the recipient will provide the same level of protection as the Principles.”
- Text from contracts related to privacy will have to be made available to the Department of Commerce upon request.

Key Changes: Onward Transfers to 3rd Parties

- Contracts with third parties must contain specific provisions limiting the processing of data by the third party.
- A company that has certified to the Privacy Shield will *remain liable* for the actions of its agents, unless it can demonstrate that it is not responsible for the violation.
  - Slight change from Safe Harbor, which had allowed companies to avoid liability so long as that company had complied with the principles.
- *Transition period:* Companies that certify to the Privacy Shield within two months of the effective date will have nine months to bring existing relationships into compliance with the Privacy Shield.

What stayed the same?

- As noted previously, much of the substance from the original Safe Harbor Principles and FAQs remained the same.
- For example, much of the text from the Safe Harbor FAQs on Pharmaceutical and Medical Products is incorporated into the Privacy Shield text:
  - The original Safe Harbor FAQ had stated that “key coded” data was not personal information within the scope of the Safe Harbor.
  - This position was widely considered dead letter in the wake of subsequent DPA interpretations of “personal data” and the Article 29 Working Party’s paper criticizing most known anonymization methods.
  - Notwithstanding those developments, the Privacy Shield retains the text of the Safe Harbor FAQ with only minor changes.

DrinkerBiddle

FTC Enforcement

FTC Privacy and Security Enforcement Program

- Leading U.S. consumer protection agency focused on commercial sector privacy
- Section 5
  - Deception – broken promises
  - Unfairness – substantial consumer injury, not outweighed by countervailing benefits, not reasonably avoidable
- Other statutes and rules
  - Gramm-Leach-Bliley Act
  - Children's Online Privacy Protection Act
  - Fair Credit Reporting Act

Privacy and Data Security Actions

- Generally administrative (no monetary remedy)
- Privacy
  - Require the creation and maintenance of a comprehensive privacy program and biennial audits for 20 years.
- Data Security
  - Require creation and maintenance of a comprehensive security program and biennial audits for 20 years by a qualified CSSLP professional or CISSP professional approved by the FTC.

FTC Safe Harbor Enforcement

- 39 Settlements
  - 36 – Deceptive certification claims
    - Lapsed certifications
    - Claimed certifications, but never applied
  - 3 – involved alleged violations of Safe Harbor Privacy Principles
- Complaints allege misrepresentation of respondents' compliance with Safe Harbor
- Orders
  - Prohibit misrepresentations about compliance with Safe Harbor

FTC Enforcement of Privacy Shield

The FTC will:

- Create a standardized referral process and provide guidance to EU Member States on the type of information that is useful in enforcement actions
- Work with EU DPAs to provide enforcement assistance
  - US SAFE WEB Act allows sharing of information
- Engage in stronger monitoring and enforcement by Department of Commerce and FTC
- Monitor compliance with existing Safe Harbor orders

When matters referred to FTC

- Review privacy policies
- Obtain further information from company or third party
- Assess whether pattern or practice of violations or significant number of consumers affected
- Enforcement action if appropriate
  - Generally administrative, no monetary relief
  - Compliance monitoring
  - Civil penalties for violations of administrative orders

DrinkerBiddle

Key Questions

Key Questions (I)

- Should companies that were previously self-certified to the Safe Harbor framework continue to maintain their Safe Harbor certification until the Privacy Shield framework becomes effective?
- If a company wishes to de-certify from the Safe Harbor framework, what does it need to do?
- If companies have begun execution of the model clauses since the invalidation of the Safe Harbor, should they continue to pursue model clauses or wait until the Privacy Shield framework becomes effective?
- If a company wishes to transition from model clauses to the Privacy Shield framework, what does it need to do?
- If a company is pursuing model contracts for the interim period before Privacy Shield becomes effective, is there language that the company should include that would enable a switch to Privacy Shield at a later date?

Key Questions (II)

- How likely is it that the Art. 29 Working Party will approve the new Privacy Shield framework?
- Will the Privacy Shield framework survive legal challenge in the EU?
- Schrems has filed legal challenges to the use of model clauses by Facebook (see http://www.europe-v-facebook.org/prism2_en.pdf). Will the model clauses survive legal challenge?

Key Questions (III)

- Will Privacy Shield requirements be interpreted in accordance with European law and the interpretations of data protection authorities, or is there more room for interpretation? For example:
  - Definition of “personal data”: Is this to be read as expansively as interpreted by EU authorities?
  - Notice: Is “actual” notice required or is posting of a Privacy Shield policy sufficient to provide “constructive” notice?
  - “Where necessary” clauses: Are these to be read strictly?
  - Legal claims and defenses: This would appear to include claims arising under US law.

Key Questions (IV)

- For companies that were previously Safe Harbor certified, what changes to their privacy programs will be necessary to comply with the Privacy Shield framework?
- Given that the EU is expected to adopt a new Data Protection Regulation in the near future, which will then go into effect in 2018, are further changes to the Privacy Shield framework, as well as to other data transfer mechanisms, expected?

DrinkerBiddle

Audience Questions