Cooley

EU-US Privacy Shield: Checklist for US Companies

July 13, 2016

Recap. On 12 July 2016, the European Commission finalised its approval of the "new and improved" EU-US Privacy Shield, which replaces the now defunct Safe Harbor scheme, declared invalid back in October 2015. You can refresh your memory on the Privacy Shield's journey:

- What's in a Name? Privacy Shield Replaces Safe Harbor
- Data Privacy Q&A: EU-US Privacy Shield

How it will work. The US Department of Commerce has announced it will accept self-certifications as soon as 1 August. Similar to its predecessor, the Privacy Shield is a voluntary, annual self-certification scheme for US organisations. By self-certifying, you pledge their compliance with data protection standards of the Shield, which are based on 16 core principles approved by the European Commission. Once an organisation commits, that commitment is enforceable under US law by either the Federal Trade Commission (FTC) or the Department of Transportation (DOT), both of which have committed to monitoring compliance.

Small print. US organisations must respond to individuals' complaints, questions and requests within 45 days of receiving a complaint. US organisations will also need to select an independent dispute resolution provider prior to self-certifying, register with that provider and make the service available to individuals.

Interested in signing up? You should at least consider it. If you do business in Europe and handle personal data, it simply makes sense. Our checklist will help you get started:

1. **Check your eligibility**
   Any US organisation that is subject to the jurisdiction of the FTC or DOT is eligible. The FTC's jurisdiction is broad and covers "acts or practices in or affecting commerce" by any "person, partnership, or corporation." There are some exceptions, for example depository institutions, insurance companies and non-profits (among others). We can help you determine whether your business model is eligible and even whether it is right for your business.
2. **It's all about the privacy policy**
   First and foremost, your handling of data must be technically and operationally compliant. Then, you must ensure your privacy policy is Privacy Shield-compliant before submitting a self-certification. For example, the policy must:
   - reflect the Privacy Shield principles and declare your organisation is Privacy Shield-compliant;
   - clearly explain to individuals how your organisation uses and discloses their personal data (don't forget this means personal data in the European sense of the word);
   - include a hyperlink to the Privacy Shield website; and
   - include a hyperlink to the independent dispute resolution provider.
3. **Verify**
   Self-certifying organisations must have procedures in place for verifying compliance, this can be done internally or externally – we can help you determine which best suits you.
4. **Be approachable**
   Organisations must provide a designated contact for handling of questions, complaints, access requests, and any other issues arising under the Privacy Shield. This can be the officer certifying compliance or another official within the organisation. If you have a Privacy Officer – even better.
5. **Ask for help**
   This checklist really just scratches the surface. Each organisation will have to examine its business model and its handling of personal data carefully before attempting to comply with the new framework. We can help you prepare for self-certification, update your privacy policy and advise on the most efficient ways to stay compliant.

Key Contacts

Ann Bevitt London	abevitt@cooley.com +44 (0) 20 7556 4264
Randy Sabett Washington, DC	rsabett@cooley.com +1 202 728 7090