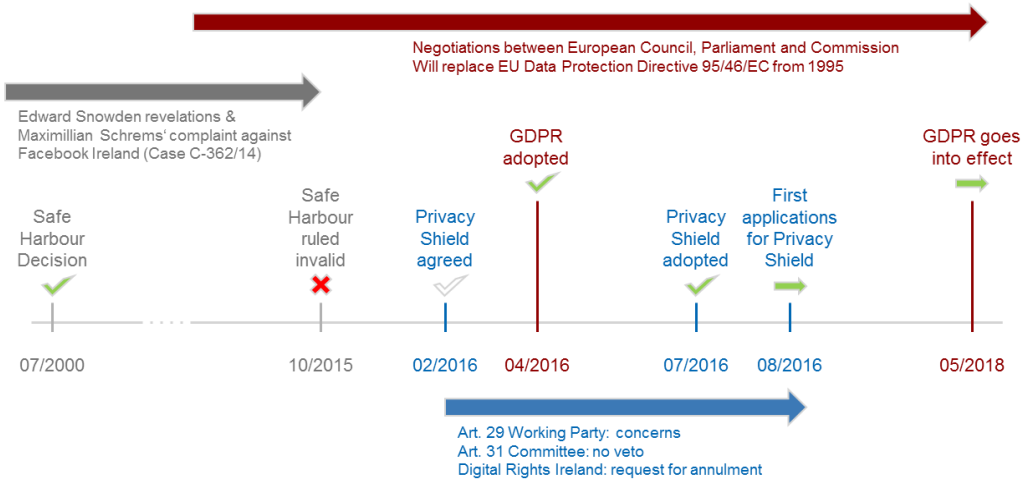
White paper

EU-U.S. framework for transatlantic exchanges of personal data for commercial purposes

Demystifying the EU-U.S. Privacy Shield – Safe Harbor, Privacy Shield & Beyond

Early in 2016, the EU-U.S. Privacy Shield started a new chapter in the history of EU-US data exchange. When the European Court of Justice declared the International Safe Harbor Privacy Principles invalid on October 6th 2015 (based on Case C-362/14), privacy and data protection issues suddenly came back into the focus of attention of the press and wider public. Shortly after, the successor to Safe Harbor ought to see the light of day.



What was Safe Harbor and why was it ruled invalid

EU Data Protection Directive 95/46/EC prohibits the transfer of personal data from EU member states to third-party countries when their data protection regulations cannot keep up with the protection levels required by EU law. This was the case for the United States of America – they do not have similar data protection regulations in place.

To serve global economic purposes and allow for transatlantic data transfers, the Safe Harbor Privacy Principles had been in place since July 2000 (Decision 2000/520/EC). The European Commission (EC) had determined that the United States "ensure[s] an adequate level of protection by reason of [its] domestic law or of the international commitments it has entered into" (acc. Article 25(6), Directive 95/46/EC). This is referred to as the Safe Harbor Decision. An important note: there is a self-certification system at the basis of Safe Harbor. In practice this means that a company self-registers their certification to signal that they comply with the Safe Harbor Privacy Principles and meet EU requirements. By complying with the required data protection standards, they may transfer data between the EU and US.

What happened next was incited by the two main characters of this play: Edward Snowden, an American whistleblower and – maybe a little less known, but definitely the decisive factor – Maximillian Schrems, an Austrian privacy activist who filed a legal complaint against Facebook Ireland.

According to the transcript of Case C-362/14, "Mr. Schrems contends in the main proceedings that United States law and practice do not ensure an adequate level of protection within the meaning of Article 25 of Directive 95/46. Mr. Schrems expresses doubts, […] concerning the validity of Decision 2000/520." After going through Austrian national courts, the case finally arrived at the European Court of Justice (EUCJ).

On the one hand, the self-certifying character of the Safe Harbor Principles may lead to skepticism. On the other hand, a much more compelling reason is the conflicting obligation imposed by US law, whereby US companies must comply with national law, whether they are part of safe harbor or not. Decision 2000/520 states that "adherence to these [Safe Harbor] Principles may be limited […] to the extent necessary to meet national security, public interest, or law enforcement requirements". Self-certified US companies are thus bound by law to outright disregard the Safe Harbor Principles when they are incompatible with these requirements and disclose personal data from EU countries when requested to do so.

Mr. Schrems contended that the laws and practices in force in the United States do "not ensure adequate protection of the personal data held in its territory against the surveillance activities that were engaged in there by […] public authorities". The most notable example is related to the Snowden revelations, which point to mass surveillance and data collection by the United States National Security Agency (NSA) and others, and warn that the extent reaches far beyond what is publicly known so far. National security and public interest had reportedly served as a justification to intercept and access data and communications of all kinds, potentially harming the fundamental rights of those whose personal data had been or is sent by corporations from the EU to the US.

On these grounds, the Court (Grand Chamber) ruled Decision 2000/520/EC, i.e. the Safe Harbor Decision, invalid on October 6th 2015. The US does not actually provide adequate protection of personal data. Also, a framework such as Safe Harbor shall not prevent a supervisory body of an EU Member State from investigating data privacy and protection complaints filed by an individual – when they are concerned about personal data being sent from an EU Member State to a third country with a controversial or inappropriate level of (data) protection.

Side note: Reform of EU Data Protection Directive 95/46/EC

The new EU data protection framework, also referred to as **General Data Protection Regulation (GDPR)**, which has been discussed and negotiated by the European Council, Parliament and Commission for roughly four years, was adopted on April 14th 2016. Regulation 2016/679 will go into effect as of May 25th 2018 and repeal Directive 95/46/EC, which has been in place since 1995. Directive 2016/680 shall be transposed into EU Member States' national law by May 6th 2018.

Key aspects include:

- Standardizing EU data protection laws across Europe
- Stronger rights and more transparent information for those whose data is collected
- US companies shall be bound by EU laws on data protection
- Increased penalties in case of violations, up to 4% of a company's worldwide annual turnover

In Germany, the Minister of Interior recently presented a second draft for adapting the national law to this new EU framework – an attempt that the German Privacy Association (DVD) values as an improvement to the first draft, but still not acceptable. They referred to it as a "data protection prevention law" rather.

The quintessence of the new EU-U.S. Privacy Shield Framework

After long, intense negotiations, the European Commission and the US Government agreed on a new framework regarding transatlantic data transfers: The EU-U.S. Privacy Shield saw the light of day. It provides a "mechanism [for companies] to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce". On July 12th 2016, the EC formally adopted the Privacy Shield Framework (Commission Implementing Decision (EU) 2016/1250), declaring it adequate to enable data transfers under EU law (see the adequacy decision).

The European Court of Justice had set forth a number of requirements on October 6th 2015, which the Privacy Shield now considers. These include effective supervision mechanisms with strong oversight, limitations for access to personal data for national security purposes, the handling and resolving of individual complaints as well as an annual joint review of adequacy decisions (MEMO/16/2462, EC Fact Sheet, July 12th 2016).

The EU-U.S. Privacy Shield resides on four pillars:

- Obligations for companies & rigorous implementation for greater transparency

  Companies self-register their participation in the Privacy Shield with the US Department of Commerce, requiring a company privacy policy in line with the Privacy Shield Principles and implying an annual renewal of their "affiliation". The US Department of Commerce subsequently monitors that they honor their commitments – if they don't, they may face sanctions or exclusion. For a list of Privacy Shield companies, go to https://www.privacyshield.gov/welcome.

Requirements of Participation: Privacy Shield Principles

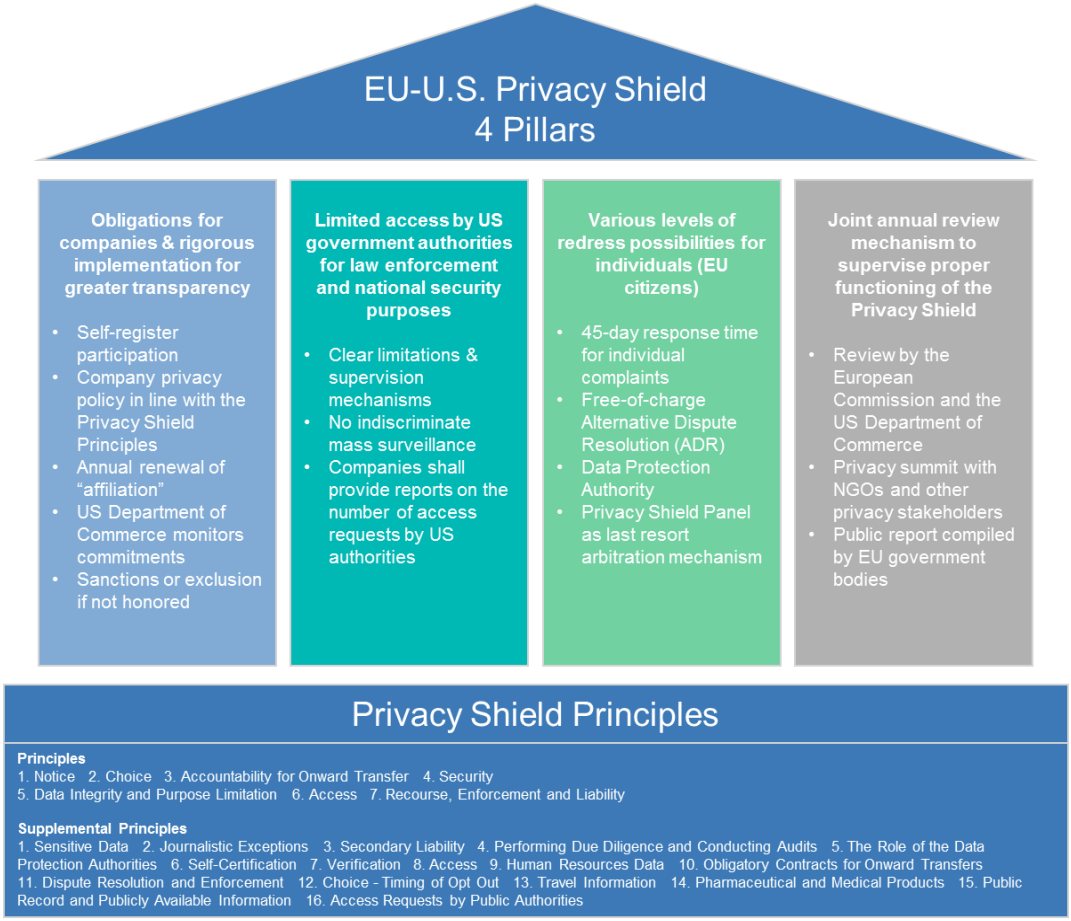
„The Privacy Shield Principles comprise a set of seven commonly recognized privacy principles combined with 16 equally binding supplemental principles that explain and augment the first seven. Collectively, these 23 Privacy Shield Principles lay out a set of requirements governing participating organizations' use and treatment of personal data received from the EU under the Framework as well as the access and recourse mechanisms that participants must provide to individuals in the EU. Once an organization publicly commits to complying with the Privacy Shield Principles, that commitment is enforceable under U.S. law.", as laid out by the US Department of Commerce on their Privacy Shield website.

Principles

1. Notice 2. Choice 3. Accountability for Onward Transfer 4. Security
5. Data Integrity and Purpose Limitation 6. Access 7. Recourse, Enforcement and Liability

Supplemental Principles

1. Sensitive Data 2. Journalistic Exceptions 3. Secondary Liability 4. Performing Due Diligence and Conducting Audits 5. The Role of the Data Protection Authorities 6. Self-Certification 7. Verification 8. Access 9. Human Resources Data 10. Obligatory Contracts for Onward Transfers 11. Dispute Resolution and Enforcement 12. Choice - Timing of Opt Out 13. Travel Information 14. Pharmaceutical and Medical Products 15. Public Record and Publicly Available Information 16. Access Requests by Public Authorities



- Limited access by US government authorities for law enforcement and national security purposes

  Access by public authorities will have clear limitations and supervision mechanisms. Indiscriminate mass surveillance shall not exist. Companies are requested to report on the approximate number of access requests by US authorities.

- Various levels of redress possibilities for individuals (EU citizens)

  These range from an individual's complaint to the company with a 45-day response time, to free-of-charge Alternative Dispute Resolution (ADR), the Data Protection Authority and – as a last resort – the Privacy Shield Panel as an arbitration mechanism.

- Joint annual review mechanism to supervise proper functioning of the Privacy Shield

  This will include a review performed by the European Commission and the US Department of Commerce, a privacy summit with NGOs and other privacy stakeholders as well as a public report compiled by EU government bodies.

Practical guidelines for US companies who receive costumer data from EU entities or partners

- Make sure to annually renew your self-certification
- Have your privacy policy in accordance with Privacy Shield Principles publicly available
- Respond to citizens' complaints as requested, within certain delays
- Co-operate and comply with EU Data Protection Authorities where needed
- Minimize amounts of collected data, make sure it gets stored only for the intended purpose(s) and no longer than needed
- Reasonably and appropriately secure data, especially when transferred to a third party (which is possible under certain circumstances)

Implications for EU citizens

- More transparency and gaining back control over one's own data
- The right to be informed about the data that is stored, to access this data and change it if necessary, and to raise a complaint, get feedback within 45 days and a cost-free (re)solution
- Redress possibilities to address access by US public authorities

Additional information for US & EU companies & EU citizens are available at European Commission: Guide EU-US Privacy Shield and US Department of Commerce: EU-US Privacy Shield.

The US Department of Commerce has started receiving applications from US companies for the Privacy Shield since August 1st 2016. More than 1,500 organizations (status January 2017) are currently listed on the US Department of Commerce Privacy Shield List, including familiar companies such as Google, Amazon or Twitter.

Who gets the most out of Privacy Shield?

This new framework is a way to keep the transatlantic transfer of data and the overall transatlantic commerce up and running. Both US and EU companies as well as public authorities and entities have an interest in continued transatlantic commerce and data exchange. EU citizens might criticize the inadequacy of this agreement and consequences for data privacy, but they also profit from it when it comes to using Social Media or international online shopping.

What is worth mentioning, however: Next to the Privacy Shield, there are alternative mechanisms which enable data transfer from within the EU to non-EU countries and thus allow US companies to receive personal data from the EU. One is governed by EU Model Contracts with Standard Contractual Clauses and the other refers to Binding Corporate Rules, such as a set of internal guidelines or a corporate code of conduct. Whether a company should certify for the new Privacy Shield or turn to one of these other mechanisms should be well-considered – Privacy Shield might not be the optimum solution for everyone, whether they have previously been part of Safe Harbor or not.

Will the EU-U.S. Privacy Shield Framework last?

The Article 29 (Data Protection) Working Party (WP29), composed of representatives of the national Data Protection Authorities (DPA), the European Data Protection Supervisor (EDPS) and the European Commission, acts as an independent advisor to the EC for what concerns their privacy and data protection matters and promotes the uniform application of Directive 95/46/EC & subsequent legislation across EU countries.

After the Privacy Shield Framework had been agreed upon in February 2016, the WP29 expressed severe concerns about its adequacy, especially with regard to the independence

of the US ombudsman and the yet broad possibilities for mass data collection. Their opinion is not legally binding and hence could not block the new framework, however, it often has an influence on EC decisions. The WP29 judgement divided opinions among business leaders and public figures, many of which publicly shared their view and arguments.

The Article 31 Committee, on the contrary, would have had a veto right, which they did not make use of. EU Member State representatives strongly supported the EU-U.S. Privacy Shield to begin in July 2016, leading to a final adoption by the EC on July 12th.

However, the Digital Rights Ireland data protection organization brought case T-670/16 to the Court of Justice of the European Union (CJEU), requesting the Court to "order the annulment of the contested decision [Commission Implementing Decision (EU) 2016/1250 of 12 July 2016] relating to the adequacy of the protection provided by the EU-U.S. Privacy Shield". It is to be seen whether the Court accepts the claim of nullity – but if so, there is a chance that the Court overturns the adequacy decision for the Privacy Shield Framework.

The on-going discussions and criticisms surrounding the EU-U.S. Privacy Shield illustrate how transatlantic data transfer is not yet secured, which leaves us curious as to the outcome. Will the CJEU challenge the Privacy Shield adequacy decision by pointing to those arguments that caused Safe Harbor to fail? How will the requirements outlined by the CJEU ruling on October 6th 2015 be fulfilled in the longer term (see here below)?

- Effective supervision mechanisms with stronger oversight by the US Department of Commerce and stronger cooperation with EU Data Protection Authorities
- Limitations for access to personal data for national security purposes, leading to no indiscriminate, mass surveillance
- Individual complaints will be handled and resolved via a number of ways, from dispute resolution by the Privacy Shield company itself to free-of-charge alternative dispute resolution solutions
- An annual joint review of adequacy decisions, monitoring the good functioning of the Privacy Shield and the commitments made in this context

Only recently did we learn that the "America first" initiative of new US president Donald Trump seems to target some essential achievements of the transatlantic cooperation, such as data protection and privacy. The Executive Order "Enhancing Public Safety in the Interior of the United States" mentions reduced data protection for non-US citizens or lawful permanent residents (Sec. 14. Privacy Act.) "to the extent consistent with applicable law". This leads to preoccupation among EU citizens and data protection authorities as well as US companies whose business model heavily relies on transatlantic data transfers. Is this going to endanger the Privacy Shield Framework including the European values it is based upon?

Last but not least, a number of changes are also ahead to insure compliance of the Privacy Shield with the new GDPR that will apply as of May 2018.

Companies are thus well advised to stay up to date with upcoming requirements and deadlines from either side – and should meanwhile have mechanisms in place to fully secure the data they handle.

Encryption – The key ingredient for businesses and owners of personal data

Let us make a simple and yet well-founded statement: To be on the safe side, EU and US companies alike need to make sure the sensitive or personal data they collect and keep is well secured. End-to-end encryption, starting as close as possible to the source of this data, is the key. This is the only way to prevent unauthorized and unwanted access – regardless of data transfers, storage locations (within EU borders, in the US or elsewhere) and applicable local laws and regulations.

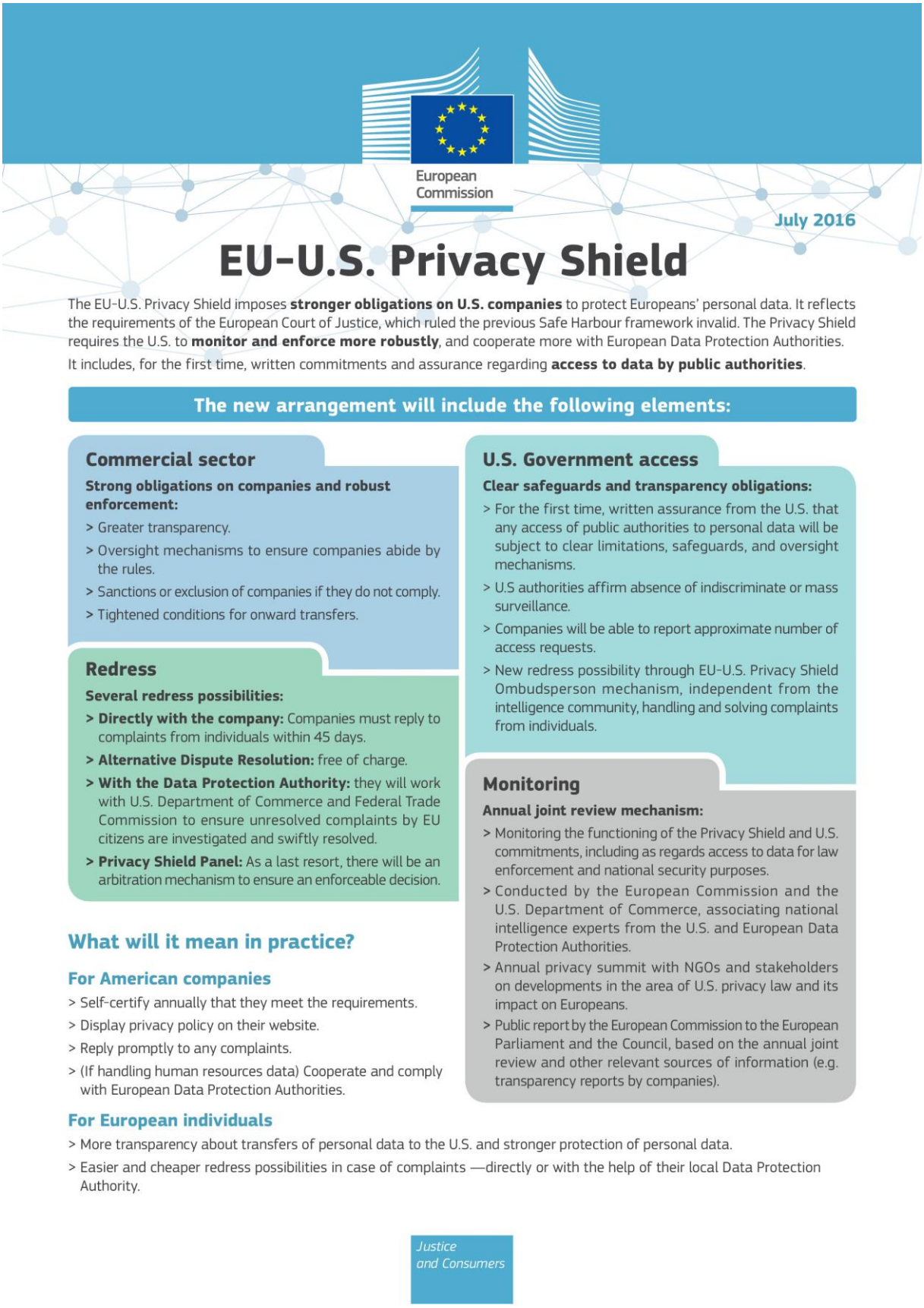
Hardware Security Modules (HSMs) and hardware encryption without backdoors prevent unwanted access to a company's sensitive data and protect data even if a breach has happened – whether initiated by cyber criminals or a public authority's mass surveillance initiative. Overall, HSMs work with true random number generation, provide encryption & decryption functionalities and allow for the secure identification and authentication of users as well as the integrity of data and code. In addition, they provide compliance with legal requirements such as FIPS 140-2 (Level 3 or even Level 4) or Common Criteria. The latest HSMs are also suitable for cloud environments where data is not physically stored on the company's own servers and multiple "tenants" access one single HSM.

To learn more about Hardware Security Modules and securely encrypting your data, no matter where it will be stored, please e-mail us at hsm@utimaco.com or call us at + 49 (0) 241 1696-200.

As a manufacturer of Hardware Security Modules, Utimaco provides the Root of Trust for your applications and related business, customer and HR data. We keep your cryptographic keys and digital identities safe to protect your critical digital infrastructures and high value data assets.

Sources of information:

* Directive 95/46/EC
* Commission Decision 2000/520/EC
* The Guardian "What is 'safe harbour' and why did the EUCJ just declare it invalid?"
* Commission Decisions on the adequacy of the protection of personal data in third countries
* Judgement of the Court (Grand Chamber) of October 6th 2015
* The end of Safe Harbor
* European Commission > Justice > Data Protection
* European Commission > Justice > Data Protection > Factsheet EU-U.S. Privacy Shield
* European Commission > Justice > Data Protection > Guide EU-U.S. Privacy Shield
* US Department of Commerce: EU-U.S. Privacy Shield
* MEMO/16/2462, EC Fact Sheet, July 12th 2016
* Neuerung der EU-Datenschutzrichtlinie
* "Datenschutzverhinderungsgesetzt", heise.de
* Foley: To join or not to join the Pricacy Shield
* European Data Protection Supervisor
* Article 29 Working Party
* Noerr - Nichtigkeitsklage gegen EU-U.S. Privacy Shield und koordinierte Prüfungsaktion der deutschen Datenschutzbehörden
* CJEU Case T-670/16
* Executive Order: Enhancing Public Safety in the Interior of the United States



Source: European Commission > Justice > Data Protection > Factsheet EU-U.S. Privacy Shield