PRIVACY SHIELD:

Your Complete Guide to Understanding & Complying

In early 2016, the EU Commission and the United States agreed on a new framework for transatlantic data flows.

Known as the EU-U.S. Privacy Shield, this new framework put stronger obligations on American companies to protect the personal data of EU citizens, and aimed to reflect the requirements set out by the European Court of Justice after it declared the previous Safe Harbor agreement invalid.

Even while the Safe Harbor agreement has been made invalid, the exact future of the Privacy Shield framework remains unclear because the EU's data protection authority, the Working Party " does not believe the agreement provides sufficient protections for EU citizens' data or safeguards against U.S. intelligence bulk data collection practices."

schellman
formerly BrightLine

WHAT HAPPENED TO THE **SAFE HARBOR AGREEMENT?**

The Safe Harbor agreement was under scrutiny for years due to the lack of enforcement, inability to address emerging risks, and a weak certification process. The agreement came into the limelight when, Maximillian Schrems, an Austrian law student, filed a complaint against Facebook after he discovered his personal data was being unlawfully processed by the company in the United States. The Court of Justice of the European Union agreed with Schrems and found the Safe Harbor agreement "compromised EU citizens' right to respect for private life, compromised the fundamental right to effective judicial protection and denied national supervisory authorities their powers to investigate breaches of the principles behind data protection."

In October 2015, the court ruled the agreement invalid, which left U.S. companies wondering if the resulting ban on transatlantic flow of data would cripple business.

PRIVACY SHIELD vs. SAFE HARBOR

Privacy Shield features broader standards than what was in the Safe Harbor agreement. Now, the EU is demanding verifiable commitment to the principles of Privacy Shield, which will likely result in a system allowing U.S. companies to certify they are in compliance with the data security and conflict resolution procedures set forth in the agreement. What's more, not complying with the principles and procedures will result in significant recourse for U.S. companies.

American companies' compliance will now be monitored directly and indirectly by an array of sources from both the United States and the EU, which could increase the regulatory risks and compliance costs for these companies.

Individuals from the EU who want to file a complaint about the use of their data now have several ways to do so under Privacy Shield.

PRIVACY SHIELD'S IMPACT ON **THE GLOBAL ECONOMY**

It has yet to be seen what effect such an agreement will have on the global economy, but with the increasing amounts and use of personal data, any restriction on access to that data could have big consequences for businesses.

After the Privacy Shield framework was released in early 2016, U.S. Secretary of Commerce Penny Pritzker said that it provides certainty that will help grow the digital economy by ensuring that thousands of European and American businesses and millions of individuals can continue to access services online.

> "Beyond being essential to transatlantic commerce, the EU-U.S. Privacy Shield also underscores the strength of the U.S.-EU relationship, it demonstrates our commitment to working together as leaders in the global economy, promoting our shared values and bridging our differences where they exist.
>
> Penny Pritzker, U.S. Secretary of Commerce

PRIVACY SHIELD BASICS

WHO WILL BE AFFECTED BY PRIVACY SHIELD?

Put simply, if your company handles or wants to handle personal data from the EU, it will have to comply with the regulations set forth in Privacy Shield. American companies handling data from the EU will have to prove they meet the requirements of the agreement, display a privacy policy on their websites, and reply promptly to any complaints they receive.

THE 6 PRIVACY SHIELD PRINCIPLES

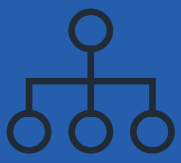
The current agreement contains six principles companies must abide by.

1 NOTICE

A company must inform individuals about:

- Its participation in Privacy Shield and provide a link to the Privacy Shield List
- The kinds of personal data it collects, how it collects the data and how it will be used
- How to contact the company with any questions or complaints about the use of data
- Any third parties the company shares an individual's data with and why it does so
- The individual's right to access his or her data
- The independent resolution body assigned to address complaints and provide appropriate recourse free of charge to the individual
- The requirement to disclose certain personal information when lawfully requested by public authorities in reference to national security or law enforcement requirements

2
CHOICE



A company must:

- Offer individuals the choice to opt out of sharing their information with a third party or if that information will be used for purposes that are materially different from those for which it was originally collected
- Obtain express affirmative consent from individuals if sensitive information like health conditions, race or religious beliefs is to be disclosed to a third party or used for purposes that are materially different from those for which it was originally collected

3
ACCOUNTABILITY FOR ONWARD TRANSFER

To transfer personal information to a third party acting as a controller, companies must:

Comply with the Notice and Choice principles and enter into a contract with the third-party controller that ensures that 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.

To transfer personal data to a third party acting as an agent, companies must: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles.

4
SECURITY

Companies creating, maintaining or disseminating personal information must:

- Take reasonable and appropriate measures to ensure it is protected from loss, misuse or unauthorized access or used for purposes that are materially different from those for which it was originally collected

5
DATA INTEGRITY AND PURPOSE LIMITATION

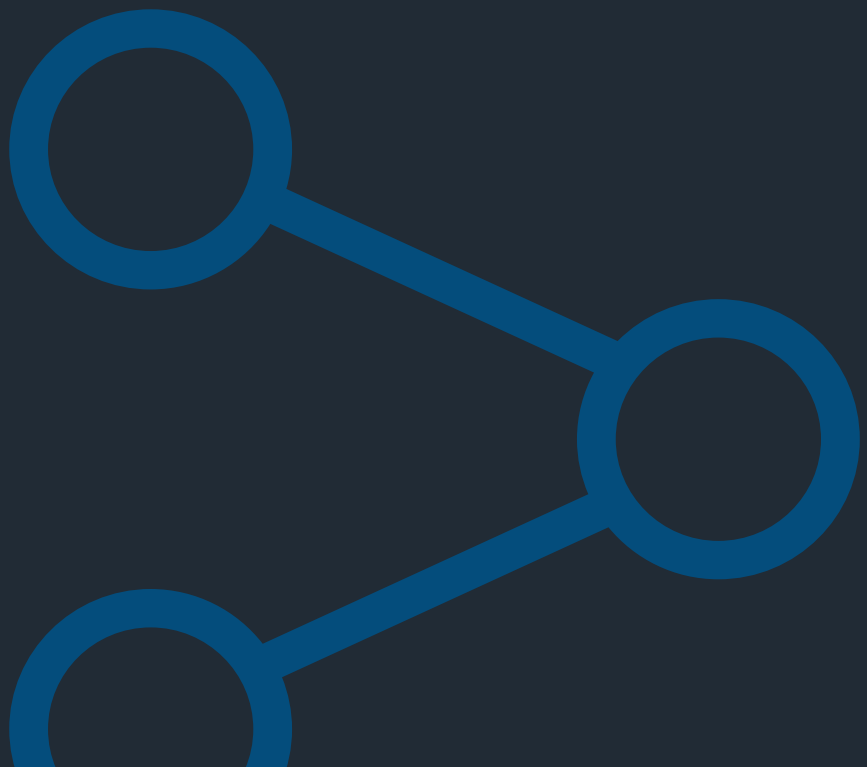
A company must:

- Not process any personal information for purposes that are not what it was originally collected for
- Ensure personal data is being used for its intended use, complete, accurate and current
- Adhere to the Privacy Shield principles for as long as it retains personal data from the EU
- Update the Privacy notice
- Notify individuals when repurposing personal data

6
ACCESS

Companies creating, maintaining or disseminating personal information must:

- Provide individuals access to any of their personal information the company holds
- Be able to amend, correct or delete information if it is inaccurate or if it has been processed in violation of the principles
- Notify individuals when repurposing personal data



COMPLYING WITH PRIVACY SHIELD:

HOW TO PREPARE FOR CERTIFICATION

A big differentiator between Privacy Shield and the now-defunct Safe Harbor agreement is that American companies now must prove they comply with the principles laid out above, and they have to do this annually.

To prove compliance, you have two options:

You can conduct a self-assessment, which must be signed by a corporate officer, or you can get external validation through an attestation from a third-party firm.

Just because Privacy Shield has not yet been approved, does not mean you should wait to get started with the certification process. There are a few things you should have in place before you begin the certification process.

THE PEOPLE

If you elect to do a self-assessment, you will need one or more subject matter experts who have a thorough legal comprehension or a thorough compliance background to look at the many conditional stipulations of the Privacy Shield and boil them down into actionable items.

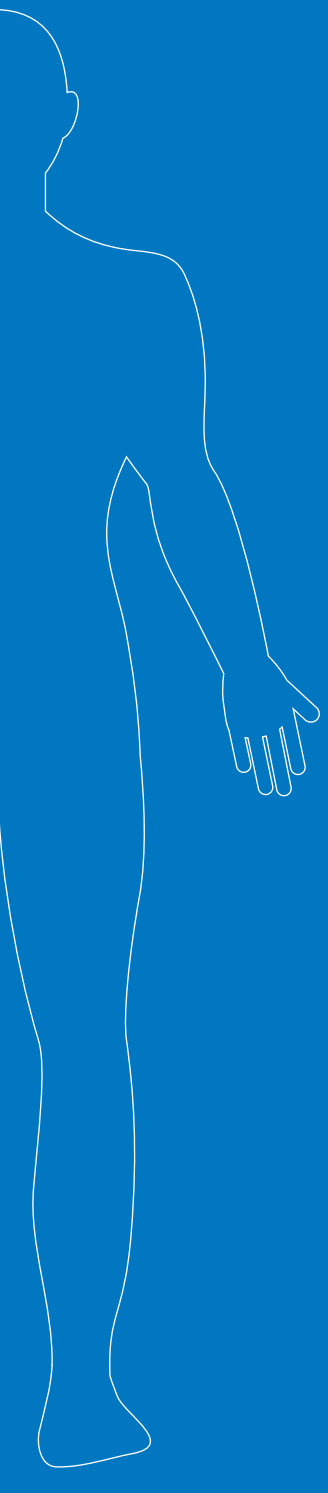
These staff members will then have to work closely with both business and IT management to examine the kind of information that's being collected and verify your processes are engineered to satisfy the new regulations.

A READINESS ASSESSMENT

A readiness assessment will provide you a cartographical analysis of your business functions and the related data inflows, housing and outflows and will outline any gaps you may have in complying with the new Privacy Shield framework.

THE ANATOMY OF A READINESS ASSESSMENT

TIME FRAME: 2-3 WEEKS



WHAT IS INVOLVED:

An IT security audit and an IT privacy audit

WHAT'S EVALUATED:

An IT security audit will evaluate the controls and processes your company has in place to maintain the integrity of information.

An IT privacy audit ensures your company has the people and technology in place to provide customers the privacy rights outlined in the six principles. In order to have sufficient privacy rights in place, your company first must have the appropriate security.

THE BENEFITS OF THIRD-PARTY ATTESTATION OVER SELF-ASSESSMENT

Involving an independent firm to certify compliance with Privacy Shield gives your company the resources it may be lacking to perform a proper assessment. Many organizations do not have the necessary experts on staff to properly interpret and implement the Privacy Shield principles.

A third-party assessor also can ensure the thoroughness and objectivity that the final Privacy Shield will likely require.

Regardless of the status of Privacy Shield, the completed framework will require most U.S. businesses to balance enterprise and accountability.

A third-party verification of Privacy Shield compliance gives your company the ability to do business with companies and individuals from the EU; provides your organization with a strong set of internal controls to operate against; offers your employees education and awareness of data and security practices; and can serve as a differentiator in the marketplace.

DON'T PUT OFF A PRIVACY SHIELD COMPLIANCE ASSESSMENT ANY LONGER.

Contact us to meet our expert assessors and get started.

schellman
formerly BrightLine