A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor":

The Easiest Way to Understand What Privacy Shield is and What You Need to Do to Use it

For more information, please contact:

David A. Zetoony
Partner
Boulder/Washington, D.C.
303 417 8530/202 508 6030
david.zetoony@bryancave.com

More than 5,000 companies had taken advantage of the now defunct U.S.-EU Safe Harbor Framework. Those companies are now considering whether to join the newly approved "Privacy Shield," and are trying to understand the difference between the old and new framework. As they do, these companies are faced with many questions: How does the Privacy Shield differ from Safe Harbor? Can you rely on the Model Clauses? Or would it make more sense to join the Privacy Shield? If so, what do you need to do to join?

To supplement our earlier publication, we have prepared a side-by-side comparison of the invalidated Safe Harbor and the new Privacy Shield. Over the next week, we will be publishing similar comparisons between Privacy Shield and other adequacy methods including the model controller-controller clauses and the model controller-processor clauses. If you would like to receive those comparisons, you can register at www.bryancavedatamatters.com:

Requirement	Safe Harbor *Invalidated*	Privacy Shield
Privacy Policy. Organization must post a privacy policy that discloses:		
Types of personal data collected.	✓	✓
Purpose for collection.	✓	✓
Contact information for questions/complaints.	✓	✓
Categories of third party onward recipients.	✓	✓
Data subject choices for limiting use.	✓	✓
Statement of compliance with program/adherence to principles.	✓	✓
Link to Department of Commerce Program List.	X	✓
The right of data subjects to access data.	X	✓
Acknowledgement of jurisdiction of FTC, DOT, or other US enforcement agency.	X	✓
Obligation to give PII in response to lawful requests from law enforcement.	X	✓
Acknowledge liability in relation to onward data transfers.	X	✓
Disclose independent recourse mechanism.	✓	✓
Ability to opt-out of onward disclosure to a third party (except for service providers), and opt-in if the information to be shared is sensitive.	✓	✓
Offer ability to opt-out of uses for materially different purposes, and opt-in if the information to be shared is sensitive.	✓	✓

Requirement	Safe Harbor *Invalidated*	Privacy Shield
Onward transfers to controllers. When transferring data to a controller the organization must:		
Enter contract stating that data can only be processed for limited and specific purposes consistent with data subject's consent.	X	✓
Require third party to notify organization if it makes a determination that it can no longer meet privacy principles.	X	✓
Onward transfers to service providers/sub-processing. When transferring data to a service provider or agent the organization must:		
Confirm service provider has subscribed to principles, is subject to Directive, is subject to another adequacy determination, or agrees to provide the level of protection in the principles by contract.	✓	✓
Take steps to evaluate provider.	X	✓
Take steps to stop unauthorized processing.	X	✓
Provide summary of contract to Department of Commerce upon request.	X	✓
Assume liability for errant processing of the service provider.	X	✓ (rebuttable presumption)
Require third party to notify organization if it makes a determination that it can no longer meet privacy principles.	X	✓
Security. Organization must implement:		
Reasonable precautions to protect from loss, misuse, unauthorized access, disclosure, alteration, and destruction.	✓	✓
Data Integrity. Organization must take:		
Reasonable steps to ensure that personal data is reliable for its intended use, accurate, complete, and current.	✓	✓
Data minimization step to retain information only for as long as it serves a processing purpose.	X	✓
Access. Organization must provide:		
Data subject's right to obtain confirmation of whether organization has data about them.	X	✓
Data subject's right to correct information about them, except when unduly burdensome to do so or third party rights implicated.	✓	✓
Data subject's right to delete information about them if inaccurate, except when unduly burdensome to do so or third party rights implicated.	✓	✓

Requirement	Safe Harbor *Invalidated*	Privacy Shield
Data Subject's Enforcement Ability. Organization must:		
Provide independent recourse mechanism that can award damages.	✓	✓
Provide independent recourse mechanism for free (as opposed to affordable).	X	✓
Accept binding arbitration.	X	✓
Accept adjudication in courts of the member state in which data exporter is established.	X	X
Accept potential liability to data subject for violation.	Unclear	✓
Contracting Party Oversight. Organization must:		
Permit data exporter to audit facilities, files, and documentation upon request to ascertain compliance with commitments.	X	X
Regulatory Oversight. Organization is required to:		
Respond to inquiries and requests from Department of Commerce.	X	✓
Respond directly to EU DPAs if human resource data is transferred.	✓	✓
Permit DPA of the member state in which data exporter is established to conduct audit.	X	X
Regulatory Liability. Organization could be liable for:		
Injunction.	✓ (FTC)	✓ (FTC)
Fines.	X	X
Implementation. Organization must provide the following to the Department of Commerce in order to self-certify:		
Contact information for organization.	✓	✓
Description of processing activities.	✓	✓
Description of privacy policy.	✓	✓
URL.	✓	✓
Effective date of privacy policy implementation.	✓	✓
Contact office for complaint handling.	✓	✓
Government entity with oversight ability.	✓	✓
Names of third party privacy programs.	✓	✓
Method of verification.	✓	✓
Independent recourse mechanism.	✓	✓
Costs.		
Fees to register	**$200**	**Unknown**