BRYAN CAVE

For more information, please contact:

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

Jena M. Valdetero
Partner
Chicago
312 602 5056
jena.valdetero@bryancave.com

OFFICES

Atlanta
Boulder
Charlotte
Chicago
Colorado Springs
Dallas
Denver
Frankfurt
Hamburg
Hong Kong
Irvine
Jefferson City
Kansas City
London
Los Angeles
Miami
New York
Overland Park
Paris
Phoenix
San Francisco
Shanghai
Singapore
Southern Illinois
St. Louis
Washington, D.C.
Affiliated Firm, Milan

A Side-By-Side Comparison of "Privacy Shield" and the Controller-Controller Model Clauses:

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

The EU Data Protection Directive 95/46/EC (the "Directive") creates the legal framework for the national data-protection laws in each EU member state. The Directive states that personal data may only be transferred to countries outside the EU when an adequate level of protection is guaranteed, and traditionally the EU does not consider the laws of the United States as "adequate" unless a company (1) enters into EU Commission pre-approved model contractual clauses with the data recipient, (2) sends data to a corporate affiliate in the US that is under the scope of "Binding Corporate Rules," or (3) entered the EU-US Safe Harbor Framework.

Most data controllers that were based in the US complied with the Directive by entering the pre-approved controller-controller model clauses or the EU-US Safe Harbor Framework. In October of 2015, the EU-US Safe Harbor Framework was invalidated by the European Court of Justice. As a result, many of the companies that had relied upon the Safe Harbor switched to the controller-controller model clauses; the use of those clauses became far and away the most popular way to comply with the Directive if you were a data controller.

On July 12, 2016, the EU formally approved a new mechanism for transferring data to the United States called the "Privacy Shield." Although you can find a full discussion of the history, and implementation, of Privacy Shield here, the best way for a company to understand Privacy Shield (and decide if it wants to use it going forward) is to do a side-by-side comparison of the Privacy Shield against the mechanism that it currently uses, used, or is considering. Our series of side-by-side comparisons has already included a Privacy Shield/Safe Harbor side-by-side comparison and a Privacy Shield/Controller-Processor Clauses side-by-side comparison.

Below, the final part of our series, is a side-by-side comparison of Privacy Shield and the express obligations contained in the controller-controller model clauses (Set II):

Requirement	Privacy Shield	Controller Obligations Under Standard Clause (Set 2)
Privacy Policy. Organization must post a privacy policy that discloses:		
Types of personal data collected.	✓	X
Purpose for collection.	✓	X
Contact information for questions / complaints.	✓	X
Categories of third party onward recipients.	✓	X
Data subject choices for limiting use.	✓	X
Statement of compliance with program / adherence to principles.	✓	X
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.	✓	X
Choice. Organization must offer data subjects the following choices:		
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.	✓	X
Offer ability to opt-out of uses for materially different purposes, and opt-in if the information to be shared is sensitive.	✓	X
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.	✓	✓ (limited to adverse changes in local laws)
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.	✓ (rebuttable presumption)	X
Require third party to notify organization if it makes a determination that it can no longer meet privacy principles.	✓	X

Requirement	Privacy Shield	Controller Obligations Under Standard Clause (Set 2)
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.	✓	X
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.	✓	✓
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.	✓	✓
Data Subject's Enforcement Ability. Organization must:		
Provide independent recourse mechanism that can award damages.	✓	X
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	✓
Accept potential liability to data subject for violation.	✓	✓ / X (data subject must initially raise issue with data exporter prior to enforcing rights against importer)
Contracting Party Oversight. Organization must:		
Permit data exporter to audit facilities, files, and documentation upon request to ascertain compliance with commitments.	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

Requirement	Privacy Shield	Controller Obligations Under Standard Clause (Set 2)
Regulatory Liability. Organization could be liable for:		
Injunction.	✓ (FTC)	✓ (Vary by DPA)
Fines.	X	✓ (Vary by DPA)
Implementation. Organization must provide the following to the Department of Commerce in order to self-certify:		
Contact information for organization.	✓	X
Description of processing activities.	✓	X
Description of privacy policy.	✓	X
URL.	✓	X
Effective date of privacy policy implementation.	✓	X
Contact office for complaint handling.	✓	X
Government entity with oversight ability.	✓	X
Names of third party privacy programs.	✓	X
Method of verification.	✓	X
Independent recourse mechanism.	✓	X
Costs.		
Fees to register	**Unknown**	**$0** (Exporter may be required to file in some states)