Bloomberg BNA

WORLD DATA PROTECTION REPORT >>>

News and analysis of data protection developments around the world.
For the latest updates, visit www.bna.com

International Information for International Business

VOLUME 17, NUMBER 2 >>> FEBRUARY 2017

European Union

Onward Transfers of Data Under the Privacy Shield: Keeping the Shield from Becoming a Sword



By Kendall Burman, Rebecca S. Eisner and Lei Shen

Companies in the U.S. that wish to import personal data from the European Union have a few adequacy options to choose from, including the EU-U.S. Privacy Shield framework. However, companies should know that certification under the Privacy Shield framework requires more than just filling out forms and providing payments. Companies that self-certify to the Privacy Shield must commit to upholding the data protection standards of the Privacy Shield, and that means ensuring that your internal practices and policies are aligned with the principles to which you certify.

The Privacy Shield framework is a successor to the U.S.-EU Safe Harbor framework, which was ruled invalid by the Court of Justice of the EU in October 2015. The invalidation of the Safe Harbor framework meant that for the approximately 4,500 companies that were relying on it for their data transfers, they had to either cease importing personal data into the U.S. or find a legally acceptable alternative mechanism. In the ab-

sence of an agreement between the U.S. and the EU, many companies turned to the standard contractual clauses issued by the European Commission for transfers to controllers or to processors, which were deemed to offer sufficient safeguards with respect to the protection of privacy and fundamental rights under EU law.

The foundation of the Privacy Shield framework, like the U.S.-EU Safe Harbor before it, are the seven core principles of data protection that companies must implement in order to certify for Privacy Shield, and to remain in compliance with it: Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; and Recourse, Enforcement and Liability. In addition to these core principles, the Privacy Shield adds 16 supplemental principles that strengthen the privacy protections of several of the core principles through heightened protections and stricter language. The Onward Transfer principle is one of the principles that have been further strengthened under the Privacy Shield.

Under the Onward Transfer principle, a Privacy Shield-certified company must ensure that certain rules are followed when transferring data onward to another controller or to a third-party agent, such as a service provider. While companies that certified for Privacy Shield before Sept. 30, 2016 have a nine-month grace period since they certified to bring their existing commercial relationships into compliance with these Onward Transfer rules, companies that are considering certifying now for the first time must be in compliance with such rules prior to certification. Either way, it is critical that these companies take the necessary actions with respect to onward transfers.

Rules for Conducting Onward Transfers

The Onward Transfer principle treats onward transfers of data to data controllers differently from onward transfers of data to a third party acting as an agent, such as a cloud service provider or other data processor. A controller is understood to be a third party who has the authority to use the information for its own purposes, whereas an agent is a third party that is acting under the instructions of the certifying company, such as an information technology service provider. The protections of the Privacy Shield continue applying to any data that were transferred under it, including to any further transfers of such data to another entity. The Privacy Shield ensures the continued protection of such data by mandating specific requirements for onward transfers of data between Privacy Shield-certified companies and third parties acting as controllers, and contracts between certified companies and agents.

The Onward Transfer principle treats onward transfers of data to data controllers differently from onward transfers of data to a third party acting as an agent.

Contracts between a Privacy Shield certified entity and a third-party controller must include the following:

- data can only be processed for limited and specified purposes consistent with the consent provided by the individual;
- the third-party controller must provide the same level of protection as the Privacy Shield principles; and
- if the third-party controller can no longer provide the same level of protection as the Privacy Shield principles, the contract must require that the controller cease processing and or take other reasonable and appropriate steps to remediate.

A Privacy Shield certified company must take the following actions with respect to a third-party agent, and while some of these steps are actions for the certified company to take, it is recommended that all of them be captured in contractual requirements binding the third-party agent:

- transfers of data must be only for limited and specified purposes;
- companies must ascertain that the agent is obligated to provide at least the same level of privacy protection required by the Privacy Shield principles;
- companies must take reasonable and appropriate steps to ensure that the data is processed by third-party agent in a manner consistent with the companies' obligations under the Privacy Shield principles;
- require that companies be notified by third-party agent if they determine they can no longer meet those obligations, and, if so, take steps to stop and remediate; and
- companies must provide a summary or a copy of the relevant privacy provisions of its contract with the Department of Commerce if requested.

To better understand the Onward Transfer principle of the Privacy Shield, it may be useful to compare this new principle with the corresponding requirements under the two other transfer mechanism with which companies are likely most familiar—the invalidated U.S.-EU Safe Harbor Framework and standard contractual clauses from the EU Commission.

   ISSN 1473-3579

Strengthened Onward Transfer Requirements Under Privacy Shield as Compared to Safe Harbor

The Safe Harbor framework included an Onward Transfer principle that required certified companies to take certain steps with regard to third parties with whom they shared their data. Similar to the Privacy Shield framework, those steps included the application of the Notice and Choice principles to third parties acting as controllers, as well as some process for ensuring that third parties acting as agents take steps to protect the data they receive. Unlike the Privacy Shield, certified companies were free to do this by confirming that the third party subscribes "to the Principles or is subject to the [EU Data Protection] Directive or another adequacy finding or enters into a written agreement. . . requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles."

The Safe Harbor framework clarified that contracts between data controllers and processors are always required and that the contract must specify the processing to be carried out and any measures necessary to ensure that the data is kept secure. The Onward Transfer principle in the Safe Harbor Framework also made clear that if a third party processes the data in a way that is contrary to the restrictions or representations of the contract, then the certified company will not be held responsible unless they knew or should have known or failed to take reasonable steps to prevent or stop such processing.

In the lead up to the invalidation of the Safe Harbor framework, representatives of the EU data protection authorities as well as the European Commission itself raised concerns over the application of the Safe Harbor principles, and asked whether there was sufficient enforcement of the Safe Harbor principles as applied to third-party agents such as cloud services providers.

The Privacy Shield framework made several changes to address those concerns. Under the Privacy Shield's Onward Transfer principle, certified companies transferring data to third-party agents are required to take reasonable and appropriate steps to ensure that the third party is processing data in a manner consistent with the Privacy Shield principles, and must require that the third party notify them if they determine they can no longer abide by those principles. And, in its principle on Recourse, Enforcement and Liability, the Privacy Shield makes clear that a certifying company has responsibility for and remains liable under the principles for data it transfers to a third-party agent for processing, unless the certifying company can prove that it is not responsible for the event giving rise to the damage. Unlike under the Safe Harbor framework, the Privacy Shield places the burden on the certifying company to prove that they were not liable for any processing of transferred data in violation of the Privacy Shield principles.

The Privacy Shield principles differ from the obligations imposed on data importers under the standard contractual clauses.

Differences Between Standard Contractual Clauses and Privacy Shield

Many companies considering certifying to the Privacy Shield may have standard contractual clauses included in their contracts with third parties for data transfers. Companies should consider carefully whether these clauses are sufficient for the purposes of satisfying the Onward Transfer principle in the Privacy Shield. In many cases, companies will need to negotiate separate and additional requirements into their third-party contracts in order to fully comply with the Privacy Shield. The Privacy Shield requires that third parties provide at least the same level of privacy protection as is required by the Privacy Shield principles, and that the information is processed by the third-party agent in a manner consistent with companies' obligations under the principles.

The Privacy Shield principles differ from the obligations imposed on data importers under the standard contractual clauses so companies certifying to the Privacy Shield may need to include different provisions in their contracts. Specifically, these contracts may need to be amended to add restrictions that are consistent with the Privacy Shield's requirements, including on further onward transfers (subcontracting), the ability to delete personal information after a change in choice by an individual, the requirement to subject the third party to audits and other verifications to ensure compliance with the Privacy Shield, and assistance in providing access to individuals for review and corrections, among others.

Concluding Tips

Separate addenda or Privacy Shield agreements may offer advantages: Companies will need to review their third-party agreements to determine how to amend them for onward transfer requirements. Unless a company has only a few agreements to review, drafting individual amendments to each third-party contract may be burdensome. You may consider drafting an addendum or Privacy Shield agreement that is intended to apply to all of your onward transfers, without specific review of each third-party agreement. The addendum or agreement should supersede prior conflicting terms, and should cover all of the onward transfer requirements in one place. For companies that have numerous third-party relationships, one agreement or addendum may be the most practical way to bring the third-party contracts into compliance, versus independent review and amendment of each third-party agreement. The single addendum or agreement has the added benefit of avoiding disclosure of the entirety of your contract with a third party on the non-Privacy Shield terms, in the event that you are required to provide a copy of your third-

party contract terms under Privacy Shield to the Department of Commerce.

Retain right to share contract: Certifying companies will want to consider including in their contract with third-party agents specific permissions to allow them to provide a copy of the relevant privacy provisions to the Department of Commerce since this is required of certifying companies if they are asked.

Track EU developments closely: Review of the Privacy Shield framework by the European authorities is baked into the language of the framework itself, allowing for annual review of how the framework's protections are implemented by certifying companies and administrative bodies. There has been much speculation over whether the Privacy Shield framework will survive such review given recent developments in both the EU and the U.S. To almost no one's surprise, the Privacy Shield, like the Safe Harbor framework before it, has been challenged in the European Court of Justice as insufficient to meet the EU's data protection standards. Suffice it to say, predicting the future of the Privacy Shield framework is difficult, and this dynamic area should be tracked closely.

   ISSN 1473-3579

  WDPR ISSN 1473-3579