NELSON MULLINS

David F. Katz | Partner
404.322.6122
david.katz@nelsonmullins.com

What You Need to Know to Get Started with Privacy Shield Certification

Reprinted with permission from Cybersecurity Law & Strategy Journal
March 1, 2017

By David F. Katz

If your company maintains operations in the European Union or is U.S. based but obtaining personal data from European citizens, you will need to strongly consider obtaining certification under the new Privacy Shield framework. Certification began in August 2016, and will make compliance with EU privacy laws when transferring data to the U.S. possible for the immediate future.

European privacy laws are considerably more stringent than those in the U.S., and the certification under the Privacy Shield is critical for businesses that want to avoid inquiries and fines in their overseas outposts. The best practices your company follows on American soil simply are not enough in the EU. American companies may regard Social Security numbers and credit card numbers as sensitive data, but in the EU, even IP addresses and geographic location data collected on phones are protected personal data. Checkout clerks in Europe do not ask for customers' phone numbers and employers cannot read workers' email. It's a different universe for privacy rights.

The EU's suspicion of data sharing is rooted in 20th century history, and it's not a good story. Whereas Americans don't give a second thought to sharing personal data in return for coupons and discounts, Europeans haven't forgotten that one of the first acts of the Nazi government was to go through the government's files on citizens and use the information to target many innocents simply based upon their political beliefs, religion or lifestyle choices. A few decades later, the Soviet-inspired Eastern Bloc elevated surveillance of ordinary citizens to a frightening new level, monitoring everything from library use to private conversations.

The memory of those times coupled with the enormous vulnerability of digital data inspired the EU's Data Protection Directive, which forbids businesses from transferring personal data from Europe to a nation outside the EU unless that country has laws ensuring protection of data at a level regarded as "adequate" by EU standards. If foreign privacy laws are not considered adequate — and they usually are not — then an international agreement can fill the gap. The basic principle asserted by the EU is that its citizens own their personal data as a natural right, and the government will enforce that right everywhere.

Since 2000, American companies have complied with the EU's Data Protection Directive through the Safe Harbor framework, an agreement worked out between the EU and the U.S. Department of Commerce. In 2015, the Court of Justice of the EU ruled that the Safe Harbor

framework was inadequate. The EU and U.S. regulatory agencies then scrambled to find a new mechanism to allow the legal transfer of information across the Atlantic. The result was the Privacy Shield, a self-certification program that is administered by the U.S. Department of Commerce and enforced by the U.S. Federal Trade Commission. The program was triggered Aug. 1, and many companies still are struggling to understand their obligations under the initiative.

Here's what you need to know to get started.

Do You Need to Be Concerned with the EU Data Protection Directive?

If you collect, use or process information that contains data about identifiable individuals in the EU, you likely are governed by the EU Data Protection Directive when you transfer that information to the U.S. While certification under the Privacy Shield is not the only avenue available for lawful data transfers, it may be the best possible way to assure European authorities and your European customers that your business is in compliance.

Any business subject to the jurisdiction of the FTC or the U.S. Department of Transportation is eligible to join the Privacy Shield. Banks and telecommunications companies are not eligible for the Privacy Shield, although they are bound by the same laws and additional restrictions that have other enforcement mechanisms.

Begin with an Assessment of Your Current Data Practices

Assemble a team of leaders in IT, HR, marketing, legal and the heads of any departments that collect or process European personal data. How does your data flow? How does it come into the organization and from where? How is it stored and who has access? Do third parties touch the data? Does the company have existing technology and processes that will allow it to comply with the privacy shield principles? How will the company monitor compliance? Privacy Shield certification is not as simple as posting the principles on the company website; there must be a means to achieve security of the data. The application of the rules is complicated and a business should strongly consider engaging outside legal experts that understand these rules and can effectively assist in designing a compliant program.

The Rules Are Enforceable in the U.S.

The FTC can fine companies $16,000 per violation per day for misrepresenting its privacy practices with respect to the collection or processing of European personal data. The legal mechanism for this is that once a company publicly announces it will adhere to the Privacy Shield principles and publishes its privacy policies, which are requirements for certification,

the FTC can then cite it for deceptive trade practices if it doesn't follow through. Once you sign on to the agreement, the data collected during that period is forever governed by the Privacy Shield and FTC enforcement, even if your company doesn't renew its certification.

The first level of enforcement is through a private recourse mechanism. The Better Business Bureau, American Arbitration Association and JAMS all have programs that meet the program's requirements and a company must set up a third-party dispute resolution process to handle complaints before being certified.

Notice and Choice

Everyone affected by your data use must be notified that you have joined the Privacy Shield and they must be apprised of the rights it affords them. These rights include knowing what data is collected, being able to review and correct it, deleting information that is inaccurate or not allowed under Privacy Shield principles and knowing the identify of third parties who can access it.

Once individuals know their rights, they are allowed choices in how their data is used. In the U.S., businesses rely on terms of service agreements that often boil down to "agree to our terms for use of your data or don't buy our product or service." Not so in the EU, where opt-in and opt- out options give consumers a menu of choices. You must make it easy for individuals to opt out of having their information shared with a third party. The EU requires an opt-in choice for anything related to health, religious or political affiliation, race and ethnicity, sexual orientation and union membership.
For both notice and choice, avoid fine print and legalese that might discourage someone from reading and understanding their rights. The burden is on the business to ensure that those affected understand their data privacy rights.

Third-Party Accountability

There is no passing the buck. A business involved in the "onward transfer" of data, such as outsourcing data processing or payroll to a third party, or that stores data in a cloud server, remains responsible for the data and is liable for noncompliance. If you touch it, you own it. A vendor must comply with Privacy Shield standards and the business that is the primary agent for the data — the Privacy Shield signatory — must include this requirement in a contract and take reasonable steps to monitor vendor compliance. Be especially vigilant in contracts with companies based in nations where neither the laws nor culture respect privacy rights.

NELSON MULLINS

Data Integrity

Organizations should be prepared to defend the need for the data they are collecting as well as its accuracy. Think of showing the need in legal terms, such as information necessary for performance of a contract or to comply with other legal obligations. More effective marketing is a weak argument. The onus to ensure accuracy of the data is on the company, even though individuals have a right to review and correct their personal data. This can be particularly problematic if a company is using data collected by another business, such as a vendor or business partner.

There are small fees attached to the certification process, but the real cost will be in setting up the internal processes for compliance. An entire industry of consultants is emerging to advise companies on certification, monitoring, resolving disputes and keeping up with changes in EU privacy laws. While Brexit will drop the UK out of the EU and perhaps encourage other nations to follow suit, don't expect those countries to reduce their privacy concerns. They are likely to continue to follow the principles of the Privacy Shield, and perhaps create their own compliance mechanisms. It is unlikely that U.S. privacy laws will ever comport with the European perspective, so transatlantic businesses should recognize that there will be no relief from these laws. The Privacy Shield, even with its costs, offers the least invasive means of compliance for most companies.

David F. Katz is a partner in Nelson Mullins Riley & Scarborough's Atlanta office where he leads the Privacy and Information Security Practice Group. He may be reached at 404-322-6122 or by email at david.katz@nelsonmullins.com.