EU: Self-certifying cybersecurity falls short

BUSINESS VIEWPOINT

Diana T. Vermeire and
Tom C. Vincent II

The Court of Justice of the European Union this fall struck down the U.S.-EU Safe Harbor framework, a mechanism whereby U.S. companies could self-certify that their data privacy measures were consistent with EU rules.

This decision by Europe's highest court has far-reaching implications for U.S. companies that collect information from EU citizens, whether customers, clients, employees or otherwise. Parties dealing with such companies may feel an impact as well.

The decision, in effect, permits EU public authorities to exercise their power to investigate and potentially suspend the collection of data from European citizens by U.S. companies. Without the protection previously provided by Safe Harbor, what will happen next is unclear.

Because of this uncertainty, U.S. companies doing business in Europe or with EU citizens should take certain steps now to ensure their data privacy measures are currently consistent with EU principles.

If you've self-certified, act like it. Any company currently self-certifying compliance with Safe Harbor should take steps to ensure that its data collection and privacy practices actually comply with the privacy practices it has previously self-certified and represented publicly.

If you're relying on another method of compliance, understand its limitations. Some companies have not self-certified compliance with Safe Harbor, instead choosing to comply via Binding Corporate Rules or Model Contractual Clauses. As an example, Safe Harbor was overturned in part because information of EU citizens in the U.S. was subject to access and review by the U.S. government, as exemplified by the National Security Agency's surveillance program. Since the Rules and Clauses similarly do not prevent government access to any EU citizen's information, they may also ultimately be found deficient.

If you're not actively complying, you have a decision to make. Companies collecting information on EU citizens — and not currently certifying under Safe Harbor or utilizing Rules and Clauses — must either begin using one of these methods, obtain the consent of the individuals whose information is being collected or reduce the specific identifying nature of the information, i.e. make it anonymous.

Whatever you're doing or relying on, confirm it's consistent with EU principles. With the increased attention that may come as a result of this ruling, every company should examine its privacy practices to ensure consistency with the general European rule that considers data protection as a fundamental human right requiring respect of a citizen's private and personal life. Recommended practices include the following, as well as relevant questions to ask to ensure they are specifically tailored to the company's business needs:

- Do people know why they are giving their information and what will happen to it? Provide notice of the type of information collected, stored and accessed, and the purpose for which it is intended to collected and used, and obtain specific and individualized consent before collecting that information.
- Is what you are asking for what you really need? Collect, store and maintain personal information only for a legitimate purpose and consistent with the reasons provided in the consent obtained at the time of collection.
- Are you only keeping it as long as you need it? Retain and store personal information for only the period necessary for the stated legitimate purpose and properly destroy it after it is no longer necessary.
- What if it's wrong? Implement a process where individuals may correct any inaccuracies in the data collected about them and may require such data be erased and destroyed.

Plan ahead. Beyond the particular overturn of the Safe Harbor, other practices permitting the sharing of EU citizen data within the U.S. are now in question, given the court's reasoning. Because of that, any business expansions into the EU or new products or partnerships with other companies should be examined in light of this uncertainty. Companies should consider not only their own internal practices, but also those of any partners when evaluating such business plans.

In addition, as requirements for data correction and/or destruction may become more stringent, system capabilities for allowing such modification should be reviewed. It is particularly important for those companies subject to Sarbanes-Oxley (SOX) to address any conflicts between SOX data preservation standards and EU data modification rights.

Given the breadth of the decision and the court's ongoing concern regarding the U.S. government's access to the personal information of EU citizens collected by U.S. companies, it remains to be seen what happens next and what options U.S. companies will have going forward. However, ensuring compliance with the basic principles identified above is a first step to complying with whatever is to come.

Diana T. Vermeire and Tom C. Vincent II are attorneys with the law firm of GableGotwals where they lead the firm's Cybersecurity and Data Privacy Group.