

September 18, 2017 | No. 12

Evolving international privacy and security laws matter to U.S.-based employers

In the global marketplace of technology, shared information and threats of identity theft, there is an ever-growing need for enhanced awareness and legal protections around the handling of personal data. In the United States, federal laws like the Health Insurance Portability and Accountability Act (HIPAA) and supplemental state-specific laws protect the fundamental right of citizens and residents to private family, home and personal communications.

Many other countries have established data protection laws or are moving quickly in that direction. In addition to protecting sensitive personally identifiable information—such as government-issued identification numbers, banking, credit and medical information—a number of laws also govern privacy regarding political affiliation, ethnicity, union participation and other human rights-based protections.

Like many U.S.-based organizations, Sedgwick's global footprint continues to grow. We are now located in multiple geographies, where different privacy and security laws apply. Additionally, our handling of claims for U.S.-based clients with employees residing in and traveling to other countries in the course of their work demands that we be aware of and comply with the applicable privacy and security laws, as well as the requirements of proper cross-border data flows to the U.S. under required controller and processor agreements. In such cases, it's important to consider where the impacted individual lives and where services are being provided, not necessarily the jurisdiction governing the claim.

EU data protection regulation takes effect May 25, 2018

On May 4, 2016, the European Union passed a new [General Data Protection Regulation](#) (GDPR); it will take effect May 25, 2018, and replace the current EU Data Protection Directive, 95/46/EC. The aims of the GDPR are to foster consistency among individual EU member countries and to add new rights, protections and requirements.

The EU GDPR will enhance obligations on matters of data subject consent, breach notification, cross-border data transfers, data anonymization or pseudonymization, profiling limitations, the right to erasure of personal information, data portability and the contractual requirements of data controllers (owners) and processors, to name a few. Large fines can be incurred for violations.

Sedgwick is closely following this important legislative change and has established a task force of expert legal, information security and operations colleagues in the U.S. and abroad to ensure our compliance—and that of our clients with claims or employees working/residing in EU member nations—by the May 25, 2018 inception date. If you have any questions or concerns regarding how the GDPR affects your claims program, please contact your Sedgwick client services representative.

[Click here](#) to read previous bulletins.

Sedgwick Claims Management Services, Inc., is a leading global provider of technology-enabled risk and benefits solutions. At Sedgwick, **caring counts**SM; the company takes care of people and organizations by delivering cost-effective claims, productivity, managed care, risk consulting and other services through the dedication and expertise of 15,000 colleagues in some 275 offices located in the U.S., Canada, the U.K and Ireland. Sedgwick facilitates financial and personal health and helps customers and consumers navigate complexity by designing and implementing customized programs based on proven practices and advanced technology that exceed expectations. For more see www.sedgwick.com.

Connect with us



© 2017 Sedgwick Claims Management Services, Inc.