Chicago Daily Law Bulletin®

Volume 163, No. 32 Serving Chicago's legal community for 162 years

Are we clear? EU clarifies upcoming personal data protection regulations

As the New Year dawned, companies on both sides of the Atlantic were probably suffering from a little data security-related hangover as a result of abrupt changes in the global privacy landscape in 2016.

The U.S.-EU Safe Harbor Framework was scrapped after the European Court of Justice in October declared it invalid as a mechanism for EU-compliant transfer of personal data from the EU to the United States.

Then came the Privacy Shield — not the first but the second attempt by the U.S. Commerce Department and European regulators to build a new mechanism to replace the Safe Harbor.

Even more change is on the way in the form of the EU General Data Protection Regulation, a wide-ranging protection and privacy law affecting companies doing business in the EU.

While the new regulation doesn't take effect until May 2018, its effects are likely to be felt this year, as companies gear up for the new regulations.

The European Parliament and the Council of the European Union passed the new regulation in April 2016. It primarily applies to businesses established in the EU but also to businesses based outside the EU that offer goods and services to or monitor individuals in the EU.

On Dec. 13, the Article 29 Data Protection Working Party, an independent European advisory body on data protection and privacy, released guidance to help businesses begin to plan their compliance with the new requirements.

The guidance focuses on explaining three particular areas of the General Data Protection Regulation that are drawing the most questions:

• The "right to data portability" requirement.

• The mandate to appoint a data protection officer.

• The requirement for member states to set up a "one-stop shop" enforcement mechanism that will allow one supervisory authority in each member state to take the lead in supervising cross-border data processing activities.

Here's an overview of the clarification contained in each of the three areas.

Right to data portability

The new regulation creates a new right to data portability, covering both data provided knowingly and actively by the consumer as well as the personal data generated by the consumer's activity. This new provision is intended to empower consumers and give them more control over their own personal information.

Specifically, the new regulation lets consumers access their personal data held by one data controller so that they can transmit the personal data to the controller of another service provider.

The right to data portability allows the direct transmission of consumers' personal data from one data controller to another, to foster both the free flow of personal data in the EU as well as competition between data controllers.

To prepare for when the new regulation takes effect in 2018, the guidance suggests that data controllers should begin developing procedures for answering data portability requests, including guaranteeing that consumers' personal data are transmitted in a structured, commonly used and machine-readable format.

Significantly, data portability only applies if the data processing is "carried out by automated means," and therefore does not apply to paper files.

Appointment of a data protection officer

Data protection officers, or DPOs, are central to facilitating compliance with the regulations under the data-protection rule, but only certain data controllers and processors need to appoint a DPO.

These include all public authorities and bodies, regardless of the type of data they process and organizations that consider monitoring individuals systematically and on a large scale or processing special categories of personal data on a large scale as one of their core activities.

While the new regulation does not define what constitutes a "public authority or body," the guidance offers examples of large-scale processing of consumer information including patient data at hospitals, individuals' travel data by a city's public transportation system via travel cards and customer data by an insurance company or bank.

But even organizations that aren't mandated to appoint a data officer may find it useful to voluntarily designate one. "[T]he DPO is a cornerstone of accountability and ... appointing a DPO can facilitate compliance and furthermore, become a competitive advantage for businesses," it points out.

Data officers serve as intermediaries between supervisory authorities, consumers and an organization's business units. Data controllers or processors will be responsible for enabling DPOs to effectively perform their role by giving them sufficient autonomy and resources.

Data officers should have expertise in national and European data protection laws and practices and an in-depth understanding of the new data protection regulation. The guidance also gives a few specifics about the professional experience or expertise needed to be a DPO but emphasizes that data officers are not personally responsible for any lack of compliance with the new regulation.

'One-stop shop' enforcement mechanism

Under the new regulation, each member state will establish an independent supervisory authority. The supervisory authority will act as the enforcement mechanism for the new privacy regulations for businesses within its establishing member state.

For companies with locations in multiple EU members states, the company will have a single supervisory authority as its lead authority. The location of the lead supervisory authority depends on the location of the data controller's "main" or "single" establishment in the EU.

It's important to note, however, that the new regulation does not permit forum shopping when it comes to lead supervisory authorities. In sum, if a company claims to have its main establishment in one member state, but no effective and real exercise of management activity or decision-making over the processing of personal data takes place in that location, the relevant supervisory authorities must decide which supervisory authority is considered the "lead."

Further, if a company does not have a location in the EU, the mere presence of a representative in a member state will not trigger the one-stop shop system.

Under the new regulation, the lead authority will coordinate any investigation as part of a "one-stop shop" enforcement mechanism in cases where a data processing operation involves the processing of a large number of individuals' personal data in a number of EU member states.

The lead authority will have the primary responsibility for dealing with a cross-border data processing activity, for example when a consumer files a complaint about the processing of his or her personal data.

Given the broad scope and generalized nature of the definitions in the new regulation, U.S. companies that collect consumers' personal data and operate in the EU shouldn't wait to ask questions or seek additional guidance on how to proceed that is specific to their situations.

U.S. companies also should examine the new regulation requirements in relation to the Privacy Shield Framework as well as their own existing data privacy policies.

PRIVACY, TECHNOLOGY AND LAW

Nerissa Coyle McGinn

Nerissa Coyle McGinn is a Chicago-based partner at Loeb & Loeb LLP. Her practice focuses on matters involving the convergence of advertising and promotions, emerging media, technology, and privacy law as well as intellectual property law, focusing on trademark clearance and counseling. She can be reached at nmcginn@loeb.com.