Published on *The National Law Review* https://natlawreview.com

New Privacy and Data Security Guidance and Rules on Tap for 2017

Article By:

Adrienne S. Ehrhardt

Regulators and agencies for a broad mix of industries issued new data security and privacy rules and guidance in the final days of 2016 and first week of 2017 that will likely shape how companies prepare for and respond to data security incidents and inquiries from data protection authorities.

State Regulatory Changes

At the state level, the New York Department of Financial Services (NYDFS) revised its proposed cybersecurity rule on December 28, 2016, and extended compliance with the rule until March 1, 2017. The changes to the rule follow extensive comments by regulated entities and include:

- A small business exception
- “Periodic” rather than annual risk assessments
- Modification of who in the organization needs to review and approve the company’s cybersecurity plan
- Easing of the requirement that companies appoint a chief information security officer
- Allowing effective alternative compensating controls to secure Nonpublic Information in lieu of encryption
- A narrowing of the events that give rise to the 72-hour breach notification requirements.

As we have noted in previous alerts, while the NYDFS’s rules apply to New York-regulated financial institutions, including insurers, money services businesses, and virtual currency companies, it is likely that New York’s rules will continue to operate as a guide for other regulators across the country.

Guidance for Federal Agencies

This week, the Office of Management and Budget (OMB) issued a memorandum setting forth

guidance for federal agencies in protecting against and responding to data security incidents, including breaches. While the memo applies to federal agencies, aspects relate to agencies' dealings with private companies, including:

- Contracts with federal contractors should include terms that allow the federal agency to take necessary steps to respond to a breach. Depending on the nature of the contract, this may result in significant obligations for those companies working with federal agencies.

- Federal grant recipients may be required to have sufficient data security protections in place. For organizations not accustomed to contemporary data security measures, this requirement may result in significant costs and/or modifications to existing data handling procedures.

Beyond these two requirements, the OMB's risk-based approach to data security may also be viewed by U.S. regulators as a road map or best practices for certain private companies guarding against and responding to data security incidents.

European General Data Protection Regulation

Finally, the Article 29 Data Protection Working Party, representatives of various European data protection authorities tasked with implementing rules related to among other things the EU-US Privacy Shield, issued new guidance on three important issues relating to:

- Data Portability: Users will have not only access to their data by data controllers but will also have the right to take that data and move it to another data controller, including competitors. The Working Party set forth guidance on the mechanisms for effectuating such portability.

- Data Protection Officer (DPO): The guidance outlines the requirements related to companies' appointment of DPOs. In some cases, a company will not need to appoint a DPO, while in other instances it is advisable and in some cases is mandatory. Those DPOs must have adequate experience for their role and must have adequate independence and resources to carry out their responsibilities.

- Identifying the Lead Data Protection Authority: For companies with multi-country operations involving data transfers, the new guidance helps identify the framework for deciding which data protection authority will be a data controller's main point of contact.

While this guidance provides some additional clarity for companies maintaining significant operations in Europe, complying with European data protection authorities' requirements remains a complicated path, as noted in our previous alerts related to the EU-US Privacy Shield (see alerts from February and August 2016).

National Law Review, Volume VII, Number 5

tap-2017