Alert

August 2, 2023

COZEN O'CONNOR

Entity-Level vs. Data-Level Exemptions in the New State Privacy Laws

Benjamin Mishkin

Member

bmishkin@cozen.com
Phone: (215) 665-2171
Fax: (215) 372-2407

Related Practice Areas

- Technology, Privacy & Data Security

Businesses operating in regulated industries, particularly in the financial services and health care sectors, need to ensure they are paying close attention to the details of the exemptions in the increasingly complex patchwork of state privacy laws. Key differences in the exemptions built into these new state laws will result in many regulated businesses having drastically divergent compliance obligations on a state-by-state basis.

The majority of the new and emerging privacy laws in the United States create entity-level exemptions for financial services entities subject to the Gramm-Leach-Bliley Act (GLBA), as well as for health care/medical services-related entities regulated by the Health Insurance Portability and Accountability Act (HIPAA). In Virginia, Connecticut, Utah, Tennessee, Montana, Florida, Texas, Iowa, and Indiana, both GLBA-regulated and HIPAA-regulated entities can avail themselves of entity-level exemptions, meaning that the entire business as a regulated entity is outside the scope of those states' privacy laws. However, privacy laws in certain other states only contain data-level exemptions for consumer financial information that is regulated by GLBA and/or for protected health information (PHI) covered by HIPAA, meaning that, although such regulated data maintained by the business will be exempt, the business as an enterprise will still need to comply with the privacy law, including making mandatory public-facing disclosures regarding the business's data collection practices and allowing consumers (and other types of individuals in California, as further noted below) to avail themselves of their statutory rights regarding their personal data that the business maintains.

Businesses have already been grappling with the exemptions in California's comprehensive privacy law, the California Consumer Privacy Act (CCPA), for several years following that law's passage in 2018 and enactment in 2020. HIPAA-covered entities can avail themselves of a wholesale entity-level exemption under the CCPA, but financial services entities subject to GLBA are only able to take advantage of the CCPA's data-level exemption for GLBA-covered consumer financial information. Financial services entities and businesses operating outside of regulated industries alike should take note that the privacy compliance hurdles in California were recently heightened by the California Privacy Rights Act (CPRA), which was passed in 2020 and went into effect at the start of 2023, as the CPRA's amendments to the CCPA removed the law's exceptions for HR-related information and business-to-business information. This means that California businesses subject to CCPA are now obligated to give employees, job prospects, former employees, and B2B contacts the same scope of rights that traditional consumers are entitled to under CCPA.

Further compounding financial services entities' compliance challenges, the financial industry will soon have a second state privacy law to grapple with, as Oregon's Consumer Privacy Act (OCPA) recently became the second privacy law in the United States with only a data-level exemption for GLBA-regulated information. The OCPA will go into effect on July 1, 2024. Although lacking an entity-level exemption for entities subject to the GLBA, the OCPA does contain entity-level exemptions for financial institutions that are regulated by Oregon's Bank Act, ORS 706.008, as well as the federal Bank Holding Company Act, 12 U.S.C. 1843(k). While many banks and bank holding companies may, therefore, still be able to avail themselves of an entity-level exemption from Oregon's law, many other GLBA-regulated entities, like alternative lenders and financing companies, will have to comply. One positive note for businesses is that, unlike the CCPA, Oregon's OCPA does contain an exemption for business-to-business information (covering information of individuals acting in a commercial context), as well as employment-related information.

Meanwhile, HIPAA-regulated businesses will also need to grapple with Oregon's OCPA, as that

law contains only a data-level exemption for PHI. Businesses subject to HIPAA will also need to pay close attention to the Colorado Consumer Privacy Act (CPA), which recently went into effect on July 1, 2023, since the CPA also contains only a data-level exemption for PHI. Lastly, Delaware's Personal Data Privacy Act (DPDPA), which is currently awaiting signature by Governor Carney, will also contain only a data-level exemption for PHI. Assuming the DPDPA is signed into law, it will go into effect on January 1, 2025. GLBA-regulated businesses can avail themselves of wholesale entity-level exemptions under both the CPA and DPDPA.

For more information and assistance regarding compliance with these new state privacy laws, please contact Benjamin Mishkin at bmishkin@cozen.com.