Delaware Joins Consumer Protection Bandwagon

On Sept. 11, 2023, Delaware became the next state to enact a comprehensive consumer data privacy law as Gov. John Carney signed the Delaware Personal Data Privacy Act (DPDPA) which will go into effect on Jan. 1, 2025. The DPDPA provides Delaware consumers with greater protections and control over their personal data while regulating entities that process such person information.

Organizations Covered

The DPDPA applies to entities that conduct business in Delaware or produce products or services that target Delaware residents and during the previous calendar year: (1) controlled or processed at least 35,000 Delaware consumers' personal data, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or (2) controlled or processed at least 10,000 Delaware consumers' personal data and derived more than 20% of their gross revenue from the sale of personal data. Notably, unlike the California Consumer Privacy Act (CCPA) and the Utah Consumer Privacy Act (UCPA), the DPDPA ***does not*** have any revenue threshold requirement that would subject an entity to the law.

Significantly, as compared to other state consumer privacy laws, such as in California, Virginia, Colorado, and Utah, Delaware's consumer threshold is low at an annual processing of 35,000 Delaware consumers' data whereas many state privacy statutes have a consumer threshold of 100,000.

Nonprofit Exemption

Nonprofit organizations and institutions of higher education will face a sea change with the DPDPA as they are not entirely exempt from the statute like many other privacy laws. The DPDPA only exempts nonprofit organizations that are committed to preventing and addressing insurance crime. Additionally, the DPDPA also exempts personal data from victims or witnesses of certain crimes, such as child abuse, domestic violence, human trafficking, sexual assault, violent felonies, or stalking collected, maintained or processed by nonprofit organizations.

Consumer Rights

The DPDPA provides consumers the right to know what personal data is being collected about them; the right to access the data; correct inaccuracies in their personal data; request deletion of personal data provided by or obtained about the consumer; obtain a copy of personal data processed by the controller in a portable and readily usable format; obtain a list of third-parties the controller has disclosed the consumer's personal data to; and opt out of the processing of personal data for the purpose of: (a) targeted advertising; (b) personal data sales; or (c) profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer. If the personal data of a child is being processed, then the parent or legal guardian may exercise the consumer rights on the child's behalf. Entities subject to DPDPA will be required to process these requests and respond to the consumer accordingly.

Under the DPDPA, “consumer” is defined as an individual who is a resident of Delaware. Moreover, the definition of “consumer” explicitly excludes any individual acting in a commercial or employment context. Thus, employee data is not covered under this law. The DPDPA also provides novel heightened protections for children, including implementing certain restrictions on the sale of data for children under the age of 18 without consent.

Sensitive Data

Notably, the DPDPA has expanded the definition of what personal data is considered “sensitive data” as compared to other privacy statutes. Following in Oregon’s footsteps, the DPDPA includes transgender and nonbinary status under the definition of sensitive data. Additionally, mental and physical health conditions, such as pregnancy, are included as sensitive data under the DPDPA.

For many institutions, the DPDPA will be another line on an ever-growing list of privacy laws with which they must comply. For some, including certain nonprofit organizations, the DPDPA will bring about a change in policy and procedure when processing personal information. Entities should begin evaluating their compliance obligations for DPDPA and working to update internal and public-facing data use policies and developing procedures to comply with this new privacy regime.

Bond attorneys regularly assist and advise clients on an array of data privacy and cybersecurity matters. Please contact Jessica Copeland, CIPP/US, Amber Lawyer, CIPP/US & CIPP/E or any attorney in Bond’s cybersecurity and data privacy practice if you have questions regarding the implementation of DPDPA and its impact on your business.

**Special thanks to Associate Trainee Victoria Okraszewski for her assistance in the preparation of this blast. Victoria is not yet admitted to practice law.*

BOND SCHOENECK & KING ATTORNEYS