Blogs
March 18, 2022
Utah Consumer Privacy Act on the Horizon

On February 25, 2022, the Utah Senate unanimously (28-0) passed Senate Bill 227, also known as the Utah Consumer Privacy Act (Privacy Act). The 2022 session adjourned on March 4, and Utah Governor Spencer Cox has 20 days from that date to either sign (or not sign) the bill, after which it becomes law, or veto the bill, in which case it does not become a law unless the legislature overrides the governor's veto. The Privacy Act would become the fourth comprehensive state consumer privacy law in the United States.

Applicability of SB 227

The Privacy Act applies to businesses that (a)(i) conduct business in Utah, or (ii) produce a product or service targeted to consumers who are Utah residents; (b) have an annual revenue of $25 million or more; and (c) satisfy one of more of certain enumerated thresholds (e.g., controls or processes the personal data of 100,000 or more consumers, or derives over 50% of gross revenue from the sale of personal data). The statute does not apply to, among others, governmental entities or third parties under contract with a governmental entity acting on behalf of that entity, institutions of higher education, nonprofits, covered entities or business associates pursuant to the Health Insurance Portability and Accountability Act (HIPAA), and information subject to HIPAA, the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, or the federal Family Education Rights and Privacy Act. Additionally, the Privacy Act does not include within its scope data that is processed or maintained in the course of employment (or an agent and independent contractor relationship). Notably, the Privacy Act also does not apply to human resources or business-to-business personal data because individuals acting in an employment or commercial context are not protected by the law.

Controller vs. Processor

Similar to the Virginia Consumer Data Protection Act and the Colorado Privacy Act, and stemming from the European Union's General Data Protection Regulation (GDPR), the Privacy Act makes a distinction between "controllers" (those who determine the purpose for processing data and are responsible for transparency, purpose specification, and data minimization) and "processors" (those who process data on behalf of a controller). In addition to determining the purpose of processing, controllers must also obtain the consumer's consent for any secondary uses, and honor consumer rights (generally within 45 days of receipt of the consumer's request). Controllers are also responsible for safeguarding data and complying with the principles of the Privacy Act such as transparency by, among other requirements, providing a privacy notice that discloses (a) the categories of personal data processed by the controller; (b) the purposes for which the categories of personal data are processed; (c) how consumers may exercise a right; (d) the categories of personal data that the controller shares with third parties, if any; and (e) the categories of third parties, if any, with whom the controller shares personal data. Processors are required to follow a controller's instructions and must enter into a contract that incorporates certain enumerated requirements (e.g., requirements pertaining to duty of confidentiality and data privacy and security safeguards) before processing data on behalf of the controller.

Consumer Rights

The bill protects "consumers" (defined as individuals residing in the state who are acting in an individual or household context, not in an employment or commercial context) and provides them with the right to access the personal data a controller processes about them, the right to delete the data they provide to controllers, the right to "port" a copy of the data a controller processes about them, and the right to opt out of the "sale" (defined as exchange by a controller to a third party for monetary consideration) of personal data or processing of personal data for targeted advertising. The parents or legal guardians of consumers who are children (defined to be

individuals under 13 years old) may exercise consumer rights on behalf of the child. The personal data of children is considered "sensitive data" under the Privacy Act, in addition to an individual's racial or ethnic origin, religious beliefs, sexual orientation, and citizenship or immigration status. "Sensitive data" also includes information regarding an individual's medical history, mental or physical health condition, or medical treatment or diagnosis by a health care professional, as well as the processing of genetic personal data or biometric data (if the processing is for the purpose of identifying a specific individual or specific geolocation data). Finally, and unlike the privacy statutes in Virginia and Colorado, which require opt-in consent, controllers are prohibited from processing "sensitive data" without first presenting the consumer with clear notice and providing an opportunity to opt out of processing.

Enforcement

As it stands, the Privacy Act does not grant litigants a private right of action and explicitly precludes consumers from using a violation of the statute to support a claim under other Utah laws. However, we know that this has not prevented plaintiffs from bringing claims adjacent to the California Consumer Protection Act under other consumer laws, so businesses should still be on the lookout for these types of lawsuits. If enacted, the Privacy Act will primarily be enforced by the Utah attorney general who, in order to bring an enforcement action, will be required to first provide the allegedly noncompliant business with (1) written notice (30 days before initiating enforcement action) and (2) an opportunity to cure (30 days from receipt of the written notice). If the Privacy Act becomes law, it will take effect on December 31, 2023.

Authors

Explore more in

Privacy & Security