

Florida Passes New Privacy Law: What It Means for Businesses

June 14, 2023

On June 6, 2023, Gov. Ron DeSantis signed S.B. 262 into law, adding Florida to the list of states passing new privacy laws this year. While much of S.B. 262 will only impact companies with annual revenues of more than \$1 billion, the law also contains provisions of broader applicability. This article summarizes S.B. 262's most notable provisions, particularly the creation of a "Digital Bill of Rights." Other than section 111.23, which prohibits governmental entities from communicating with social media platforms to request content moderation, the law takes effect on July 1, 2024.

Impact on Certain Businesses With Annual Gross Revenues of Over \$1B and Businesses That Process Personal Information on Their Behalf

The Digital Bill of Rights imposes familiar rights and requirements on companies with annual gross revenues over \$1 billion AND that (i) derive 50% or more of those revenues from the sale of online advertisements; (ii) operate a consumer smart speaker; or (iii) operate an app store or a digital distribution platform offering at least 250,000 different software applications ("controllers"). Those rights and requirements will, by virtue of the threshold noted above, only apply to very large companies, including privacy notices, data protection assessments, required contractual provisions between controllers and processors, rights to access, know, correct, and delete, and an expanded set of opt-out rights, including the right to opt out of (a) the collection and processing of sensitive or biometric data (e.g., data collected through voice and facial recognition technology) and (b) the use of their personal data for purposes of targeted advertising, data sales, and certain profiling. The Digital Bill of Rights also contains some familiar exemptions; for example, financial institutions, nonprofits, and covered entities or business associates subject to HIPAA are exempt from the law.

The Digital Bill of Rights also impacts businesses that process personal information on behalf of controllers ("processors"). For example, processors must execute a contract governing the processing to be performed on behalf of the controller, including a description of the parties' legal obligations and a retention schedule for the deletion of nonexempt personal information. Other obligations imposed on processors more closely align with those set forth in other state privacy

laws, including requiring the processor to adhere to the controller's instructions and assist in responding to consumer rights requests.

The law does not create a private right of action but can be enforced by the Florida attorney general.

Impact on Businesses Predominantly Accessed by Children

In addition to creating the Digital Bill of Rights, for providers of an online service, product, game, or feature **likely to be predominantly accessed by individuals under 18** ("online platforms"), S.B. 262 generally:

- Prohibits processing personal information that "may result in substantial harm or privacy risk to children";
- Limits profiling children unless certain conditions are met; and
- Restricts online platform's collecting, selling, sharing, using, and retaining of children's personal information, especially precise geolocation data.

Impact on Other Businesses

More broadly, S.B. 262 expands the Florida Data Breach Notification Statute's definition of "personal information" to include Floridians' biometric data or geolocation paired with an individual's name or initials and bars the sale of sensitive personal information, without prior consent, by any for-profit business in the state that collects data about consumers. For these instances, the business must post a notice on its website, stating: "This website may sell your sensitive personal data." While the definition of "sensitive data" is narrow, it includes an individual's race, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; certain genetic or biometric data; personal data collected from a known child; and precise geolocation data.

Takeaways and Next Steps

Based on the above, companies collecting or processing the personal information of Floridians should evaluate which of S.B. 262's provisions apply to them, and how, and consider what adjustments may be advisable for compliance, such as changing practices related to children's personal information, revising incident response plans to reflect the expanded definition of "personal information," etc.

Authored By



John E. Clabby



Patricia M. Carreiro



Eden Marcu

Related Practices

[Technology](#)

[Cybersecurity and Privacy](#)

Related Industries

[Technology](#)

©2024 Carlton Fields, P.A. Carlton Fields practices law in California through Carlton Fields, LLP. Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.