



Florida Likely to Join Growing Trend with Digital Bill of Rights: Top 9 Questions for Businesses

Insights

5.12.23

Florida is expected to be the tenth state to pass comprehensive consumer privacy legislation. The Florida Digital Bill of Rights was approved by the state legislature earlier this month and is expected to soon be signed by Governor Ron DeSantis and take effect on July 1, 2024. The proposed law will apply to certain controllers and data processors, and includes protections regarding biometric data, the collection of data by smart speakers, and protections for minors. The Florida bill further demonstrates that businesses must adapt to new consumer privacy rights and keep up with pending legislation that is advancing across the country. California, Connecticut, Colorado, Indiana, Iowa, Utah, Virginia, Montana, and Tennessee have already enacted similar laws. Additionally, more than a dozen other states are considering consumer privacy legislation. For now, here are the answers to your top nine questions about Florida's pending Digital Bill of Rights.

1. What Are the Key Requirements of the Bill?

The proposed law will apply to controllers that gross more than \$1 billion a year and:

- make at least 50% of their revenue from the sale of advertisements online;
- operate an app store or digital distribution platform that offers at least 250,000 different software applications for consumers to download and install; or
- operate a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud-computing service that uses hands-free verbal activation (that's you, Siri!).

If signed into the law, the new legislation will provide consumers with rights similar to those provided by other states' existing consumer privacy laws, including the right to opt out of the sale of their personal information, to see the data a company has about them, and to request that their personal information be deleted or corrected.

The bill also creates requirements for individuals who process personal data on behalf of a controller. The definition of "processor" — unlike that of controllers — is not limited to businesses that generate more than a certain amount of revenue, but instead includes "a person who processes personal data on behalf of a controller."

2. Will the Florida Digital Bill of Rights Apply to Your Business?

Unless you are a processor or generate more than \$1 billion in global gross annual revenue, no. The proposed law applies only to (1) processors, regardless of size, and (2) controllers that meet the conditions noted above. Additionally, affiliates of companies that meet the requirements of the Florida Digital Bill of Rights will be required to comply. An affiliate is defined as an entity that controls or is controlled by or is under common branding with another legal entity.

The statute exempts non-profits, government entities, institutions of higher education, financial institutions, data governed by the Gramm-Leach-Bliley Act (GLBA), covered entities or business associates and information and data subject to the Health Insurance Portability and Accountability Act (HIPAA), and information governed by the Family Educational Rights and Privacy Act (FERPA).

3. Are Employees Treated as Consumers Under the Florida Law?

No. The bill expressly states that the term “consumer” does not include an individual acting in an employment context. This contrasts with the California Consumer Privacy Act (CCPA), which treats all employees and job applicants as consumers. Florida’s legislation aligns with other recently passed state consumer privacy laws with respect to employment-related data. Notably, the exemption for employee data is a permanent provision in the Florida bill.

4. Does the Law Cover Information Collected in the B2B Context?

No. The bill states that the term “consumer” does not include individuals acting in a commercial context. This also differs from the CCPA but is similar to the laws of other states that have enacted their own consumer privacy laws.

5. Can Individuals Sue for Violations of the Florida Digital Bill of Rights?

No. The state attorney general has exclusive authority to enforce the law, and there is no private right of action that would allow individuals to sue for a violation. The proposed law also states that a violation cannot serve as the basis for any lawsuit under any other law, tort, or contract. This should eliminate the risk of an unfair business practice claim based on a violation of this law. However, individuals can submit complaints and report violations to the state — and consumer complaints may trigger an investigation.

6. What Rights Do Consumers Have Under the Florida Law?

Consumer rights include:

- the right to access data;
- the right to request the deletion of data;
- the right to correct data;

- the right to correct data;
- the right to data portability for data previously provided by the consumer;
- opt-out rights for the purpose of targeted advertising, the sale of personal data, and profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer;
- the right to revoke consent; and
- the right to appeal if a consumer's request is denied.

A controller is required to respond to a consumer request within 45 days of receipt. The controller may extend the response by 15 days if reasonably necessary. If a controller cannot take action regarding the consumer's request, the controller must inform the consumer without undue delay and provide a justification for the inability to take action on the request. A controller must also provide instructions for how to appeal its decision regarding a consumer's request and establish a conspicuously available process for consumers to appeal.

7. What Does the Florida Digital Bill of Rights Require of Processors?

A processor is required to adhere to the instructions of a controller and assist the controller in meeting or complying with the controller's duties pursuant to the Florida Digital Bill of Rights. For example, a processor is required to assist the controller in responding to consumer rights requests, assist with the security of processing personal data and notification of a breach of security of the processor's system, and providing necessary information to enable the controller to conduct and document data protection assessments.

Additionally, the contract between the controller and processor must include clear instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, the rights and obligations of both parties, and a requirement that the processor ensure each person processing personal data is subject to a duty of confidentiality.

Processors must also delete or return all personal data to the controller as requested, make available to the controller all information to demonstrate compliance with the Florida Digital Bill of Rights, allow reasonable assessments by the controller, and engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor.

8. What Are the Penalties for Failing to Comply?

The Florida Department of Legal Affairs can assess a civil penalty of up to \$50,000 per violation. Civil penalties may also be tripled if the violation involves a Florida consumer who is known to be a child, is based on the failure to delete data or correct personal information after receiving a request when an exception does not apply, or is based on continuing to sell or share a consumer's personal data after the consumer chooses to opt out.

9. What Should Businesses Do in the Meantime?

Businesses subject to the Florida Digital Bill of Rights should take immediate action to develop the capabilities and policies to ensure compliance. Companies should consider the following actions: conduct a privacy gap assessment, create a reporting mechanism, prepare appropriate privacy policies, hire and train employees to respond to requests, and create an appeal procedure.

Need More Help?

For further information, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney on the firm's [Consumer Privacy Team](#). Fisher Phillips will continue to monitor the progress of this legislation and any enforcement efforts and will provide updates as warranted, so make sure that you are subscribed to [Fisher Phillips' Insight System](#) to get the most up-to-date information direct to your inbox.

Want to learn more? [Register for our upcoming webinar](#): The U.S. Data Privacy Landscape – Current State of Play. Join Risa Boerner (CIPP/US, CIPM), Usama Kahf (CIPP/US), and Anne Yarovoy Khan from the Fisher Phillips Consumer Privacy Team for a deep dive on data privacy regulations currently in effect and set to take effect across the US.

Related People



Risa B. Boerner, CIPP/US, CIPM

Partner

610.230.2132

Email





Brett P. Owens

Partner

813.769.7512

Email

Service Focus

Privacy and Cyber

Consumer Privacy Team

Related Offices

Fort Lauderdale

Orlando

Tampa