THOMPSON HINE

Privacy & Cybersecurity Update

November 2023

Florida's Digital Bill of Rights and Breach Notification Amendment

The list of states with their own general purpose privacy statutes has again grown. On June 6, Governor Ron DeSantis signed into law the Florida Digital Bill of Rights (FDBR), which provides Florida residents a broad range of data protection rights and requires certain covered businesses to comply with new data privacy and information security requirements. The law becomes effective on July 1, 2024.

Most notably, the FDBR does not create a private right of action. Rather, the Florida Department of Justice will have exclusive authority to enforce the law and penalties, which could range up to $50,000 per violation, subject to trebling for violations related to certain categories of personal data and incidents of noncompliance with the law.

Scope of applicability. The FDBR applies to controllers that either conduct business in the state or produce a product or service used by residents of the state, and that process or engage in the sale of personal data. In this sense, the FDBR's scope is narrower than other states' privacy laws.

In addition, the FDBR defines a "controller" more narrowly than similar data privacy laws. It defines a covered controller as a business that collects personal data about consumers, determines the purpose and means of processing, makes in excess of $1 billion in global gross annual revenue, and satisfies at least one of the following:

- Derives 50% or more of its global gross annual revenue from the sale of online advertisements, including providing targeted advertising or selling ads online.
- Operates 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.
- Operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

Under the FDBR, personal data is defined as "any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual." The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. Personal data, however, does not include deidentified data or information that is publicly available.

The FDBR defines **"sensitive data"** as personal data that reveals an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, citizenship or immigration status, personal data of a known child, genetic or biometric data, or precise geolocation data (i.e., information derived from technology that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet).

The FDBR includes several exemptions that are standard in data privacy frameworks, including exemptions for data processing activities governed by federal law (e.g., HIPAA, GLBA) and data processing conducted in the employment and business-to-business contexts. It also exempts data used solely for measuring or reporting advertising performance, reach, or frequency.

Consumer data privacy rights. The FDBR provides consumers residing in Florida with the following rights:

- The rights to confirm whether a controller is processing the consumer's personal data and to access the personal data.
- The right to correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.
- The right to delete *any or all* personal data provided by or obtained about the consumer.
- The right to obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a *digital* format.
- The right to opt out of the processing of the personal data for purposes of targeted advertising, the sale of personal data or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer.
- The right to opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data
- The right to opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

The FDBR defines a *"***sale of personal data"** as the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. However, the sale of personal data does not include the disclosure of personal data to data processors and other common data disclosure practices (e.g., disclosure of personal data to an affiliate, at the request of a consumer, or as part of a corporate restructuring).

The FDBR creates a framework for how controllers must receive, authenticate, and respond to consumer data privacy requests and mandates that a company "establish a process" to allow a consumer to "appeal" a controller's refusal to take action on a data rights request within a reasonable period of time after the consumer receives the decision.

In particular, a controller must establish two or more secure, reliable, and conspicuously accessible methods for consumers to exercise their data privacy rights, which must include a mechanism on the controller's website for consumers submit a data rights request. In addition, a controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal data may also provide an email address for the submission of requests.

With respect to appealing a controller's decision, the FDBR specifies that the process must be "conspicuously available and similar to the process" for submitting data privacy rights requests. The FDBR requires controllers to inform consumers in writing of any action taken or not taken in response to an appeal, including the reason or reasons for the decision.

Privacy policies and other notices. Controllers are required to provide consumers with a "reasonably accessible and clear privacy notice, *updated at least annually*" that describes their data processing activities (e.g., categories of personal data collected and processed, purposes of processing, categories of personal data shared with third parties). The notice must also describe how consumers can exercise their data privacy rights, including how they can appeal a controller's decision. A controller that sells personal data or uses it for targeted purposes has the additional obligation to "clearly and conspicuously disclose" such processing and how consumers can exercise their opt-out rights. The FDBR prescribes specific language that controllers that engage in the sale of "sensitive data" and "biometric data" must provide in their privacy policies:

- For sale of sensitive personal data: "NOTICE: This website may sell your sensitive personal data."
- For sale of biometric data: "NOTICE: This website may sell your biometric personal data."

Processor obligations and contracts. The FDBR places affirmative obligations on processors, such as those related to adhering to a controller's instructions and assisting the controller in responding to consumer rights requests, compliance with the security of processing, and notification of a security breach in the processor's system.

Like many other data protection laws, the FDBR also requires controllers and processors to execute written agreements that contain certain data protection clauses,

which must address, among other things, clear instructions for processing data, the nature and purpose of data processing, duration of the processing, the type of data subject to processing, parties' rights and obligations, and a duty of confidentiality.

The FDBR requires these controller-to-processor contracts to include clauses requiring the processor to delete or return the personal data in its custody at the end of the data processing services unless retention is required by law. In addition, the FDBR mandates written contracts between processors and subcontractors that require the subcontractor to meet the processor's obligations with respect to personal data processing.

Data protection assessments. The FDBR requires a controller to conduct and document a data processing assessment when engaging in a variety of common business activities, such as targeted advertising, selling of personal data, processing of sensitive data, and certain types of profiling. The assessment must be made available to the Florida attorney general upon request. This section applies to processing activities generated on or after July 1, 2023.

Rewards programs and anti-discrimination. The FDBR, like other state data protection laws, permits controllers to offer consumers different services or similar services at different prices that are related to loyalty or rewards programs. However, a controller may not discriminate against a consumer for exercising a data privacy right (e.g., by denying the consumer a good or service or charging a different price or rates or by providing a different level of quality of a good or service).

Consent. The FDBR limits how a controller can use personal data without a consumer's consent. For example, a company may not "process personal data for purposes that are neither reasonably necessary to, nor compatible with, the disclosed purposes for which such personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent." A controller is also prohibited from processing sensitive data or personal data for the purposes of sale or targeted advertising without obtaining appropriate consent.

Data security requirements. The FDBR places affirmative data security obligations on controllers to protect the confidentiality, integrity, and accessibility of personal data. It requires them to establish, implement, and maintain reasonable administrative, technical, and physical data security practices to protect the confidentiality, integrity, and accessibility of personal data appropriate to the volume and nature of the personal data at issue.

Breach Notification Amendment

The FDBR also carves out an amendment to the state's breach notification law. As background, Florida's breach notification law requires certain organizations to disclose to affected individuals and the Florida Department of Legal Affairs a "breach of security," defined as an unauthorized access of data in electronic form containing personal information. requirements related to information security and breach notification. The amendment expands the definition of "personal information" subject to breach notification to individuals and the state.

Under the state's breach notification law, "personal information" is more *narrowly* defined than the term "personal data" under the new FDBR law. It means an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (i) a Social Security number; (ii) a driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (ii) a financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (iv) any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (v) an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. Personal information also includes a username or email address, in combination with a password or security question and answer that would permit access to an online account.

The FDBR amendment adds to this definition **(vi) an individual's biometric data and (vii) any information regarding an individual's geolocation.** Biometric data under the breach notification law takes on the same meaning as defined under the FDBR. It is data generated by automatic measurements of an individual's biological characteristics including fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. This change will go into effect on July 1, 2024.

FOR MORE INFORMATION

For more information, please contact:

Thomas F. Zych
216.566.5605
Tom.Zych@ThompsonHine.com

Thora Knight
212.908.3971
Thora.Knight@ThompsonHine.com