# Florida Digital Bill of Rights (FDBR) Summary

On June 7, 2023, Governor Ron DeSantis (R) signed SB 262, the "Florida Digital Bill of Rights" (FDBR) into law. The Act's provisions take effect on July 1, 2024. Note that SB 262 also contains provisions relating to government moderation of social media and children's protections. A non-comprehensive summary of significant privacy-related elements of the Act follows:

| | |
|---|---|
| **Covered Entities** | The **Florida Digital Bill of Rights (FDBR)** applies to a sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements: (i) is organized or operated for the profit or financial benefit of its shareholders or owners; (ii) conducts business in Florida; (iii) collects personal data about consumers, or is the entity on behalf of which such information is collected; (iv) determines the purposes and means of processing personal data about consumers alone or jointly with others; (v) makes more than $1 billion in global gross annual revenues; and (vi) satisfies at least one of the following: (a) derives 50% or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online; (b) 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; or (c) operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install. |
| **Covered Data** | ***"Personal information"***: 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. The term does not include deidentified data or publicly available information.<br><br>***"Sensitive data"***: a category of personal data that includes any of the following: (a) personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status; (b) genetic or biometric data processed for the purpose of uniquely identifying an individual; (c) personal data collected from a known child, or; (d) precise geolocation data. |
| **Key Definitions** | ***"Consent"***: a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative act.<br><br>***"Dark Pattern":*** a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice and includes, but is not limited to, any practice the Federal Trade Commission refers to as a dark pattern.<br><br>***" De-Identified Data"***: data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual.<br><br>***"Pseudonymous Data"***: any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.<br><br>***"Targeted Advertising"***: displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time across affiliated or unaffiliated websites and online |

| | |
|---|---|
| | applications used to predict the consumer's preferences or interests. The term does not include an advertisement that is: (a) based on the context of a consumer's current search query on the controller's own website or online application; or (b) directed to a consumer search query on the controller's own website or online application in response to the consumer's request for information or feedback.<br><br>***"Sale of Personal Data"***: the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include any of the following: (a) the disclosure of personal data to a processor who processes the personal data on the controller's behalf; (b) the disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer; (c) the disclosure of information that the consumer intentionally made available to the general public through a mass media channel and did not restrict to a specific audience, and; (d) the disclosure or transfer of personal data to a third party as an asset that is part of a merger or an acquisition. |
| **Consumer Rights** | • **Access:** A consumer has the right to confirm whether a controller is processing the consumer's personal data and to access the personal data.<br>• **Affirmative Consent:** A controller may not process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with the Children's Online Privacy Protection Act.<br>• **Correction:** A consumer has 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.<br>• **Deletion**: A consumer has the right to delete any or all personal data provided by or obtained about the consumer.<br>• **Portability:** A consumer has 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.<br>• **Opt Out Rights**: A consumer has the right to opt out of the processing of the personal data for purposes of: (i) targeted advertising; (ii) the sale of personal data; or (iii) profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer. A consumer may also opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data and the collection of personal data collected through the operation of a voice recognition or facial recognition feature. |
| **Business Obligations** | • **Responding to Consumer Requests**: A controller shall respond to a consumer request without undue delay, which may not be later than 45 days after the date of receipt of the request. The controller may extend the response period once by an additional 15 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension. A consumer has the right to a free response up to twice annually. The controller bears the burden of demonstrating the manifestly unfounded, excessive, repetitive, or technically unfeasible nature of any denied requests and may charge the consumer a reasonable fee to cover such administrative costs of complying with the request or may decline to act on such requests. A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process must be conspicuously available at no cost to the consumer and similar to the process for submitting requests to initiate action pursuant to this section. Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing of any action taken in response to the appeal, including a written explanation of the reason or reasons for the decision.<br>• **Data Minimization**: A controller shall limit the collection of personal data to what is adequate, |

| | |
|---|---|
| | relevant, and reasonably necessary in relation to the purposes for which such data is processed.<br>• **Avoid Secondary Use**: A controller shall not process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.<br>• **Data Security**: for purposes of protecting the confidentiality, integrity, and accessibility of personal data, establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.<br>• **No Unlawful Discrimination:** A controller shall not process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers. A controller shall not discriminate against a consumer for exercising any consumer rights.<br>• **Transparency**: A controller shall provide consumers with a reasonably accessible and clear privacy notice, updated at least annually that includes all of the following information: (a) the categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller (b) the purpose of processing personal data; (c) how consumers may exercise their rights including the process by which a consumer may appeal a controller's decision with regard to the consumer's request; (d) if applicable, the categories of personal data that the controller shares with third parties; (e) if applicable, the categories of third parties with whom the controller shares personal data; and (f) a description of the methods by which consumers can submit requests to exercise their consumer rights. If a controller engages in the sale of personal data that is sensitive data, the controller must provide the following notice: "NOTICE: This website may sell your sensitive personal data." If a controller engages in the sale of personal data that is biometric data, the controller must provide the following notice: "NOTICE: This website may sell your biometric personal data."<br>• **Purpose Specification:** A controller may not process personal data for purposes other than those specified. Personal data processed by a controller may be processed to the extent that the processing is: (a) reasonably necessary and proportionate to the purposes specified; (b) adequate, relevant, and limited to what is necessary in relation to the specific listed purposes; and (c) done to assist another controller, processor, or third party with the purposes specified.<br>• **Disclosure**: A controller shall clearly and conspicuously disclose the sale of personal data to third parties or processing of personal information to third parties for targeted advertising in addition to the manner in which a consumer may exercise the right to opt out of such activity. |
| **Data Protection Assessments** | A controller shall conduct and document a data protection assessment for certain processing activities of consumer personal data. Data protection assessments must identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by the safeguards that can be employed by the controller to reduce the risks. The assessment must factor in the following: (a) the use of de-identified data; (b) the reasonable expectations of consumers; (c) the context of the processing; and (d) the relationship between the controller and the consumer. |
| **Controller / Processor Distinction** | • **A processor shall adhere to the instructions of a controller and assist the controller** in meeting or complying with the controller's duties under FDBR. A contract between a controller and a processor shall govern the processor's data processing procedures with respect to processing performed on behalf of the controller.<br>• The contract must include requirements that the processor: (a) ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data; (b) at the controller's direction, delete or return all personal information to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law; (c) make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance; (d) allow, and cooperate with, reasonable |

| | |
|---|---|
| | assessments by the controller or the controller's designated assessor; and (e) engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data. |
| **Exceptions and Exemptions** | • A controller may disclose pseudonymous data, deidentified data, or aggregate consumer information with an exercise of reasonable oversight to monitor compliance with any contractual commitments and shall take appropriate steps to address any breach of the contractual commitments.<br>• FDBR shall not be construed to restrict a controller's or processor's ability to: (a) comply with laws; (b) comply with inquiries by government authorities; (c) prepare for and defend legal claims; (d) provide a product or service requested by a consumer; (e) protect interests essential for life or physical safety of the consumer; (f) prevent, detect and protect against security incidents; (g) preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security; (h) engage in scientific or statistical research in the public interest.<br>• Data exempt from FDBR includes: protected information under HIPAA, the Health Care Quality Improvement Act of 1986, the Patient Safety and Quality Improvement Act, the Fair Credit Reporting Act, the Driver's Privacy Protection Act of 1994, FERPA, the Farm Credit Act, any licensed insurance company, and COPPA. |
| **Enforcement** | • FDBR does not establish a private cause of action.<br>• A violation of FDBR is considered an unfair and deceptive trade practice solely by the Department of Legal Affairs. If the Department has reason to believe that a person is in violation, the Department may bring an action against such person for an unfair or deceptive act or practice. The Department may collect a civil penalty of up to $50,000 per violation. Civil penalties may be tripled for any of the following violations: (a) a violation involving a Florida consumer who is a known child. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age; (b) failure to delete or correct the consumer's personal data after receiving an authenticated consumer request or directions from a controller to delete or correct such personal data, unless an exception to delete or correct such personal data applies; (c) continuing to sell or share the consumer's personal data after the consumer chooses to opt out.<br>• **Right to Cure**: After the Department notifies a person in writing of an alleged violation, the Department may grant a 45-day period to cure the alleged violation and issue a letter of guidance. The Department may consider the number and frequency of violations, the substantial likelihood of injury to the public and safety of person or property in determining whether to grant the 45-day cure period. If the alleged violation is cured to the satisfaction of the Department and proof of such cure is provided, the Department may not bring an action for the alleged violation but in its discretion may issue a letter of guidance that indicates that the person will not be offered a 45-day cure period for any future violations. |