

The FDBR (effective July 1, 2024) governs certain entities that control (“controllers”) or process (“processors”) and, as applicable, sell, the personal data of Florida residents, other than in the employment or business-to-business contexts (“consumers”). It also grants Florida residents certain rights with respect to their personal data.

Applicability

The FDBR primarily is aimed at big tech companies. The FDBR applies to companies that meet the following criteria or control or are controlled by a company that meets the following criteria:

1. operates for profit;
2. conducts business in Florida;
3. collects personal data about consumers or is the entity on behalf of which such information is collected;
4. determines the purposes and means of processing personal data about consumers alone or jointly with others;
5. makes in excess of **\$1 billion** in global gross annual revenues; and
6. 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.

Practical Application for Businesses

Consumer Rights:

- 1) **Right to Access:** the right to confirm whether a controller is processing personal data and access such data.
- 2) **Right to Correct:** the right to correct inaccuracies in the consumer’s personal data.
- 3) **Right to Delete:** the right to delete personal data concerning the consumer.
- 4) **Right to Data Portability:** the right to obtain the personal data in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another entity without hindrance, provided the controller will not be required to reveal any trade secret.
- 5) **Right to Opt Out:**
 - a) the processing of personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling for decisions that significantly affect a consumer;
 - b) the collection or processing of sensitive data;
 - c) the collection of personal data through the operation of a voice recognition or facial recognition feature.

Controller Obligations:

- Publish a privacy notice that is reasonably accessible and clear and includes the necessary details, including disclosures for the sale of sensitive personal data or biometric data on the business website.
- Obtain consent to collect sensitive data, including personal data of any consumers under **13**, and for use of voice recognition or facial recognition features (or similar features).
- Act on consumer requests within **45 days**; provide notice of extensions and the appeals process as necessary.
- Enter into binding data processing agreements with requisite limitations for third-party processors.
- Conduct and document an impact assessment for the processing of personal data for purposes of (i) targeted advertising, (ii) the sale of personal data, or (iii) profiling for decisions that significantly affect a consumer.

Penalties:

- The Florida Attorney General has exclusive enforcement authority. A violation of the FDBR could result in civil penalties up to **\$50,000 per violation, but these may be tripled in certain circumstances.**
- The Florida Attorney General may grant an optional 45-day cure period to correct a violation.