HINSHAW

Alerts

Florida and Texas Businesses Must Comply With Updated Privacy Regulations Effective July 2024

July 16, 2024

If you are a business operating in the Sunshine and/or Lonestar state, then this alert is for you. As discussed further below, Florida recently issued regulations, effective **July 18, 2024**, clarifying certain requirements set forth in the Florida Digital Bill of Rights (FDBR), which went into effect on July 1, 2024.

Texas has also been quite busy. Even before the **July 1, 2024**, effective date of its comprehensive privacy law, the Texas Data Privacy and Security Act (TDPS), its Attorney General, Ken Paxton, was busy demonstrating his and the state's commitment to protecting consumer privacy. Read below to find out how these updates may apply and impact your business.

Florida

Who Does the Law Apply to?

The FDBR targets a narrow type of business, *i.e.*, those with more than $1 billion in annual sales obtained primarily (more than 50 percent) from online ads. It also applies to companies that operate voice-activated smart speakers and large-scale app stores.

That means that only a handful of companies will be subject to the FDBR. However, there is one rule that *all* businesses must follow. Pursuant to section 501.715, all businesses must obtain prior consent from a consumer before selling that consumer's sensitive data. If your company is subject to the FDBR, then you should be aware of the recently issued regulations.

Authorized Persons

Previously undefined in the FDBR, the regulations now define an **"authorized person"** as:

- A consumer whose data is processed or sold by a controller or processor;
- A person granted express, written authority by a consumer to act for the consumer in exercising the consumer's rights;
- A person granted authority to act for a consumer under a power of attorney, whether denominated an agent, attorney in fact, or otherwise. The term includes an original agent, co-agent, and successor agent; or

Attorneys

Jason J. Oliveri

Service Areas

Privacy, Security & Artificial Intelligence

©2024 Hinshaw & Culbertson LLP

- A person who is a parent or legal guardian of a child who is exercising the rights granted to the child or to the parents of a child.

An authorized person who is authenticated is entitled to act on a consumer's behalf to exercise all rights and protections granted to them under the FDBR.

Authenticating Consumer Requests

The regulations also provide that upon receipt of a request to exercise consumer rights and prior to taking any action or providing a response, covered businesses must use a commercially reasonable method to authenticate the consumer.

In the case of a person submitting a request on behalf of another, covered businesses should use a commercially reasonable method to authenticate the individual and determine whether they are an authorized person. In determining whether a method of authentication is commercially reasonable, covered businesses must consider:

- The rights the requester is seeking to exercise;
- The type, sensitivity, value, and volume of personal data at issue;
- The degree of possible harm that could be suffered by the consumer in the event of improper access, use, or deletion of their personal data; and
- The cost to the business.

These authentication practices must also be followed when a covered business refuses a request and the consumer, or someone acting on their behalf, appeals. Covered businesses should avoid requesting additional data to authenticate and should not require a fee.

Data Security

Security is another key topic covered by the regulations. Required **"general data security practices"** pursuant to the regulations include:

- Protecting the confidentiality, integrity, and accessibility of personal data from unauthorized access, use, disclosure, deletion or modification;
- Maintaining data security practices that comply with the risk management framework and standards adopted by the National Institute of Standards and Technology (NIST);
- Considering the volume and nature of the personal data being processed or sold;
- Establishing, implementing, and maintaining the security practices for the most sensitive type of data within a data set with mixed levels of sensitivity;
- Establishing, implementing, and maintaining data security practices for personal data not subject to an exemption by the controller or processor after the satisfaction of the initial purpose for which such information was collected or obtained until the personal data has met its retention schedule; and
- Establishing, implementing, and maintaining procedures for the secure disposal of personal data.

"Administrative data security practices" are also covered and include, but are not limited to:

- Establishing, implementing, and maintaining effective organizational controls for personal data;
- Designation of a qualified individual responsible for overseeing and implementing data security practices, as required by the FDBR;
- Regularly testing and monitoring compliance with data security practices, including key controls, systems, and procedures, to detect actual and attempted attacks or intrusions; and
- Limiting access to the systems containing personal data to authenticated users who have been trained and tasked with performing those duties.

©2024 Hinshaw & Culbertson LLP

Covered entities must also implement technical and physical data security practices in place, including encryption. "Unencrypted storage of personal data on mobile electronic devices and passive storage media is prohibited."

Enforcement

With respect to enforcement, the regulations provide that a consumer who files a complaint with the Department of Legal Affairs (the "Department") must provide certain information in the complaint, including:

- The consumer's name, address, telephone number, email address, and any user name or identity with the controller;
- The authorized person's name, address, telephone number, email address, and relationship with the consumer if an authorized person is submitting a complaint on their behalf;
- The controller's name and website; and
- A description of all the actions the consumer or authorized person requested the controller to take in connection with consumer rights.

The rule also provides that a covered business that employs a "reasonable age verification 'method' regularly used by the government or businesses for the purpose of age and identity verification" cannot be found by the Department to have willfully disregarded the child's age.

Reasonable parental verification is also required before any consumer right can be exercised. In sum, the regulations make clear that when it comes to consumer rights, covered businesses must authenticate and verify using commercially reasonable methods.

Texas

As reported here, Attorney General Paxton has announced plans to aggressively enforce, among other actions, the state's data broker law. This law requires that covered businesses register with the Texas Secretary of State by filing a registration statement and paying a $300 fee.

True to his word, the Attorney General began an enforcement sweep at the end of June, noticing over 100 companies of their alleged failure to register as data brokers.

The intensity of the sweep, and those that will surely follow in light of the **July 1, 2024**, effective date for the TDPS, reflects not only Paxton and the state's commitment to consumer privacy but also a broader initiative to hold data brokers accountable. To avoid penalties and fines, not to mention the possibility of reputational damages, covered businesses should act quickly and seek to comply if they have not already done so.

©2024 Hinshaw & Culbertson LLP