

The Rhode Island Data Transparency and Privacy Protection Act



Marc J. Soss, Esq.
FL Estate Planning
Lakewood Ranch, FL

“This requires entities to clearly disclose data collection practices, provide mechanisms for consumers to access, correct, and delete their personal data...”

On June 25, 2024, in response to concerns about data privacy and security in our digital age (how personally identifiable information is shared by businesses), the governor of Rhode Island transmitted a comprehensive privacy bill (SB 2500/ HB 7787), the Rhode Island Data Transparency and Privacy Protection Act (DTPPA), back to the state legislature. The Rhode Island Legislature enacted the DTPPA on July 1, 2024. Effective on January 1, 2026, the DTPPA provides privacy policy requirements to any commercial website conducting business or offering products and services to Rhode Island residents. The DTPPA does not apply to employee or business-to-business personal data.

The DTPPA applies to businesses that operate both inside and outside the state and collect information from Rhode Island residents who visit their websites. The law requires businesses to obtain explicit consent before collecting or sharing sensitive personal information and imposes strict guidelines for data breach notifications. This includes a retail business that collects names, email addresses, and purchase histories from its Rhode Island customers and those that store or analyze its data.

The DTPPA defines “personal data” as “any information that is linked or reasonably linked to an identified or identifiable human.” This includes names, addresses, email addresses, phone numbers, social security numbers, IP addresses, bank account information, medical information, and biometric and geolocation data.

Application

The DTPPA applies to: (i) any operator of a commercial website or internet service provider conducting business in Rhode Island or with Rhode Island customers. This applies regardless of the size of the company; and (ii) any for-profit entity that conducts business in Rhode Island or provides products or services targeted to Rhode Island residents and, during the immediately preceding calendar year, either: (a) controlled or processed the personal data of at least 35,000 Rhode Island customers; or (b) controlled or processed the personal data of at least 10,000 Rhode Island customers and derive more than 20% of their gross revenue from the sale of personal data.

The law further requires companies to fulfill

multiple critical obligations: (i) Transparency; (ii) Consumer Rights; (iii) Consent (explicit, informed consent from consumers); (iv) Data Security (security measures to protect personal information from unauthorized access), breaches, and other security threats; and (v) Breach Notification (prompt notification of affected consumers and relevant authorities in the event of a data breach). This requires entities to clearly disclose data collection practices, provide mechanisms for consumers to access, correct, and delete their personal data, implement procedures for consumers to easily opt-out of data collection and sharing, and allow a customer to request a company provide a copy of the customer’s personal data.

Sensitive Data

The DTPPA list of sensitive data includes racial or ethnic origin, religious beliefs, mental or physical health condition or diagnosis, sex life, sexual orientation, or citizenship or immigration status. It further precludes the processing of biometric or genetic information for the purpose of unique identification, the personal data of a known child (under 13), or precise geolocation data.

Non-Compliance

Companies found in violation of the DTPPA may face:

- (i) **Financial Penalties:** A violation “shall constitute a deceptive trade practice and result in fines between \$100 and \$500 per disclosure.
- (ii) **Legal Actions:** Non-compliance may result in a lawsuit from affected consumers and potential class-action litigation.
- (iii) **Reputation Damage:** Failing to adhere to the standards may result in reputation damage, loss of consumer trust and potential loss of business.
- (iv) **Operational Disruptions:** Compliance failures may result in increased scrutiny from regulators.

The Bar Journal assumes no responsibility for opinions, statements, and facts in any article, editorial, column, or book review, except to the extent that, by publication, the subject matter merits attention. Neither the opinions expressed in any article, editorial, column, or book review nor their content represent the official view of the Rhode Island Bar Association or the views of its members.

FLORIDA LEGAL ASSISTANCE



Marc J. Soss, Esquire

Estate Planning
Probate Administration
Probate Litigation
Elder Law
Corporate Law
Real Estate Closings

(941) 928-0310
mjs@fl-estateplanning.com
www.fl-estateplanning.com

**IF YOU WANT TO
PRACTICE LAW,
WITHOUT WORRYING
ABOUT YOUR BUSINESS...**

YOU'RE IN LUCK.

As a Rhode Island Bar Association member benefit, Red Cave Consulting provides **FREE** business management consulting services for Rhode Island attorneys. Red Cave has consulted with 3000+ law firms in the past 10 years. Put our experience to work for you.



CALL: (617) 398-7181
EMAIL: JARED@REDCAVELEGAL.COM

Or visit the Bar website's Law Practice Management page to get started.

Enforcement

Rhode Island's attorney general has exclusive enforcement power, there is no private right of action, and the law does not contain a right to cure provision. Penalties can be up to \$10,000 per violation under Rhode Island's unfair and deceptive trade practices statute.

Exempt Businesses and Agencies

Government entities, nonprofit organizations, institutions of higher education, financial institutions subject to the Gramm-Leach-Bliley Act (GLBA), national securities associations, and covered entities or business associates under the Health Insurance Portability and Accountability Act (HIPAA) are exempt from the DTPPA requirements. The DTPPA also exempts data subject to HIPAA, the Fair Credit Reporting Act, the GLBA, the Driver's Privacy Protection Act, the Family Educational Rights and Privacy Act, and the Farm Credit Act.

Obligations

The DTPPA requires all businesses to provide a website privacy policy, in a conspicuous location, on its website or online service platform that includes (i) all categories of personal information that are collected; (ii) all third parties to whom personal information has or may be sold; (iii) an active email address or other mechanism for a consumer to contact the company; and (iv) if the company engages in targeted advertising, disclosures about that processing. It is important to note that the law does not extend to offline collection, and there is no requirement to identify the purpose of the processing or the categories of personal data the controller shares with third parties.

In addition to the privacy policy requirements, entities that meet the size threshold of the DTPPA must adhere to the following obligations: (i) limiting the collection of personal data; (ii) the establishment, implementation and maintenance of administrative, technical and physical data security practices; (iii) customer consent before processing sensitive data; and (iv) a non-discrimination policy.

The DTPPA additionally requires controllers to conduct a data protection assessment for each of the following activities: (i) processing personal data for targeted advertising; (ii) selling personal data; (iii) processing sensitive data; and (iv) processing personal data for purposes of profiling.

Customer Requests

Under the DTPPA, data controllers must respond to a request within 45 days after receipt, with a 45-day extension available as reasonably necessary. If denied, the controller must provide a method to appeal the denial of a request and make the process conspicuously available. ♦