2022 Legislative Session
Data Privacy
Timing and Process

• Week 2 of Session (Ends March 10th)
• HB 9 – Consumer Data Privacy by Rep. McFarland
  • Session Priority for Speaker Sprowls
  • Committee References
    • Commerce
    • Judiciary

• SB 1864- Consumer Data Privacy by Sen. Bradley
  • Committee References
    • Commerce and Tourism Committee
    • Regulated Industries
    • Rules
Data Privacy Legislation Key Points

- **Creates Right to Know** – Gives consumers the right to know what information a business has collected about them.

- **Creates Right to Delete** – Allows consumers to request to delete or correct certain personal information, unless the information is crucial to maintaining the person’s account.

- **Creates Right to Opt-Out of Sale** – Requires businesses to allow consumers to “opt-out” of the sale or sharing of personal information to third parties, giving consumers more control over their personal information.

- **Requires Certain Privacy Procedures to be Followed** – Requires businesses to let consumers know how their personal information will be collected, stored and disseminated.

- **Limits Retention of Personal Information** – Limits a business’ internal use and how long it keeps personal information.
HB 9 – Data Privacy by Rep. McFarland

• Defines a “Controller” as a sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:
  • Is organized or operated for the profit or financial benefit of its shareholders or owners; Does business in FL; Collects personal information about consumers, or is the entity on behalf of which such information is collected.
  • Satisfies two or more of the following thresholds:
    • Has global annual gross revenues in excess of $50 million;
    • Annually buys, receives, sells, or shares the personal information of 50,000 a year; or
    • Derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.

• Requires certain controllers to publish a privacy policy for personal information.

• Defines “personal information” as information that identifies or is linked or reasonable linked to an identified or identifiable consumer or household, including biometric information and unique identifiers. The term does not include public information that is readily available to the public from government records, certain employee information, or deidentified or aggregate information.

• Gives consumers certain rights related to personal information collected by a controller, including:
  • The right to access personal information collected,
  • The right to delete or correct personal information, and
  • The right to opt-out of the sale or sharing of personal information.

• Requires controllers to comply with certain consumer requests and make certain information available on the controller’s website.

• Requires a controller that receives a verifiable consumer request to access, delete, correct, or opt-out must comply with such consumer request, with certain exceptions.

• Effective July 1, 2023
• The bill does not restrict any controller or third party’s ability to:
  • Collect and transmit personal information that is necessary for the sole purpose of sharing such personal information with a financial service provider to facilitate short term, transactional payment processing for the purchase of products or services.
  • Comply with federal, state, or local laws.
  • Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.
  • Cooperate with law enforcement agencies concerning conduct or activity that the controller, processor, or third party reasonably and in good faith believes may violate federal, state, or local law.
  • Exercise legal rights or privileges.
• Collect, use, retain, sell, or disclose deidentified personal information or aggregate consumer information. If a controller uses deidentified information, the controller must:
  • Implement technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;
  • Implement business processes that specifically prohibit reidentification of the information;
  • Implement business processes to prevent inadvertent release of deidentified information; and
  • Not attempt to reidentify the information.
HB 9 Exclusions

• The bill does not apply to the following:
  • Information collected by a controller or processor pursuant to a written contract between the controller and processor.
  • Information used by a controller or processor to advertise or market products or services that are produced or offered directly by the controller or processor as long as personal information is not sold, shared, or disclosed to another party outside the consumer’s direct interaction with the controller or processor.
  • Information collected by a controller acting in the role of a job applicant, employee, owner, director, officer, contractor, volunteer, or intern of the controller, to the extent the personal information is collected and used solely within the context of the person’s role or former role with the controller.
  • Information de-identified in accordance with HIPPA and its associated rules;
  • Information protected for purposes of HIPPA and its associated rules;
  • Information collected as part of a clinical trial or research that is subject to the Federal Policy for the Protection of Human Subjects or other specific industry guidelines;
  • Information collected, processed, or sold or disclosed pursuant to the Fair Credit Reporting Act;
  • Information collected, processed, sold, or disclosed pursuant to GLBA and its implementing regulations;
  • A financial institution as defined in GLBA to the extent the financial institution maintains personal information in the same manner as nonpublic personal information, and as long as such financial institution does not use personal information for targeted advertising in conjunction with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception;
  • Information collected, processed, sold, or disclosed pursuant to DPPP;
  • Education information covered by FERPA;
  • Information disclosed to respond to alert of a present risk of harm to person or property, fraud, or illegal activity;
  • Information disclosed when a consumer uses or directs a controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party.
SB 1864: Data Privacy by Sen. Bradley

• Defines a “Controller” as a sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:
  • Is organized or operated for the profit or financial benefit of its shareholders or owners; Does business in FL or provides products/services to residents of FL; Collects personal information about consumers, or is the entity on behalf of which such information is collected.
  • Satisfies either of the following thresholds:
    • Controls processing of personal information of 100,000 or more consumers not exempt; OR
    • Controls or processes personal information of at least 25,000 consumers not exempt and derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.
• Requires certain controllers to publish a privacy policy for personal information.
• Defines “personal information” as information that identifies or is linked or reasonable linked to an identified or identifiable consumer. The term does not include public information that is readily available to the public from government records, certain employee information, or deidentified or aggregate information.
• The Act grants consumers the right to:
  • Opt-out of the sale of their personal information;
  • Know what personal information a business has collected about them;
  • Delete their personal information;
  • Correct their personal information;
  • More stringently control the sale of their minor child’s personal information.
• Requires controllers to comply with certain consumer requests and make certain information available on the controller’s website.
• Requires a controller that receives a verifiable consumer request to access, delete, correct, or opt-out must comply with such consumer request, with certain exceptions.
• Effective December 31, 2022
SB 1864 Exclusions

The bill provides express exemptions from the bill for the following types of information:

- Collected or disclosed by a business in the scope of its role as an employer or similar relationship regarding its employees, agents, independent contractors, owners, directors, officers, applicants, interns, or volunteers;
- Part of a written or verbal communication or a transaction between the controller or processor and the consumer solely within the context of the business conducting due diligence regarding providing or receiving a product or service;
- Collected by a business, service provider, or third party regarding employment or benefits;
- Collected by a business that enters into a contract with an independent contractor and disclosers personal information to fulfill contract;
- De-identified in accordance with HIPPA and its associated rules;
- Collected as part of a clinical trial or research that is subject to the Federal Policy for the Protection of Human Subjects or other specific industry guidelines;
- Collected, processed, or sold or disclosed pursuant to the Fair Credit Reporting Act;
- Collected, processed, sold, or disclosed pursuant to GLBA and its implementing regulations;
- Collected, processed, sold, or disclosed pursuant to the Farm Credit Act and its implementing regulations;
- Collected, processed, sold, or disclosed pursuant to DPPP;
- Education information covered by FERPA;
- Collected, processed, sold, or disclosed relating to the price, route, or service by entities that are subject to the federal Airline Deregulation Act;
- Vehicle Information or ownership information that is retained by or shared between a new motor vehicle dealer and the vehicle’s manufacture, if done so to effectuate a warrantied vehicle repair or recall.
Private Right of Action and FDUTPA

**Private Right of Action (HB 9 Only)**

- The bill allows a Florida consumer to bring a civil action against a controller, processor, or person for the following:
  - Failure to protect a consumer’s nonencrypted and nonredacted personal information or e-mail address, in combination with a password or security question and answer that would allow access to the consumer’s account, and is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a controller’s violation of the duty to implement and maintain reasonable security procedures and practices;
  - Failure to delete or correct a consumer’s personal information after receiving a verifiable consumer request, unless the controller qualifies for an exception to requirements to delete or correct; or
  - Continuing to sell or share a consumer’s personal information after the consumer chooses to opt-out.

- The bill allows a court to grant the following relief to a consumer:
  - Damages in an amount not less than $100 and not greater than $750 per consumer per incident, or actual damages, whichever is greater.
  - Injunctive or declaratory relief.
  - Upon prevailing in a civil action, the consumer may recover reasonable attorney’s fees and costs.

**FDUTPA (HB 9 and SB 1864)**

- If DLA has reason to believe that any controller, processor, or person is in violation of the requirements of the bill, DLA may bring an action against such controller, processor, or person for an unfair or deceptive act or practice under FDUTPA. A consumer may not bring an action under FDUTPA under the bill.
GET SOCIAL

Online at https://cccfla.com/
@CapCityConsult

CONTACT US

Chris Schoonover
P | 850.264.7588
E | chris@cccfla.com
A bill to be entitled
An act relating to consumer data privacy; creating s. 501.173, F.S.; providing applicability; providing definitions; requiring controllers that collect a consumer's personal data to disclose certain information regarding data collection and selling practices to the consumer at or before the point of collection; specifying that such information may be provided through a general privacy policy or through a notice informing the consumer that additional specific information will be provided upon a certain request; prohibiting controllers from collecting additional categories of personal information or using personal information for additional purposes without notifying the consumer; requiring controllers that collect personal information to implement reasonable security procedures and practices to protect the information; authorizing consumers to request controllers to disclose the specific personal information the controller has collected about the consumer; requiring controllers to make available two or more methods for consumers to request their personal information; requiring controllers to provide such information free of charge within a certain timeframe and in a certain format upon receiving a verifiable consumer request;
specifying requirements for third parties with respect to consumer information acquired or used; providing construction; authorizing consumers to request controllers to delete or correct personal information the controllers have collected about the consumers; providing exceptions; specifying requirements for controllers to comply with deletion or correction requests; authorizing consumers to opt out of third-party disclosure of personal information collected by a controller; prohibiting controllers from selling or disclosing the personal information of consumers younger than a certain age, except under certain circumstances; prohibiting controllers from selling or sharing a consumer's information if the consumer has opted out of such disclosure; prohibiting controllers from taking certain actions to retaliate against consumers who exercise certain rights; providing applicability; providing that a contract or agreement that waives or limits certain consumer rights is void and unenforceable; providing for civil actions and a private right of action for consumers under certain circumstances; providing civil remedies; authorizing the Department of Legal Affairs to bring an action under the Florida Unfair or Deceptive Trade Practices Act and to adopt rules; requiring the department to
submit an annual report to the Legislature; providing report requirements; providing that controllers must have a specified timeframe to cure any violations; providing jurisdiction; declaring that the act is matter of statewide concern; preempting the collection, processing, sharing, and sale of consumer personal information to the state; amending s. 501.171, F.S.; revising the definition of "personal information"; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:

Section 1. Section 501.173, Florida Statutes, is created to read:

501.173 Consumer data privacy.—
(1) APPLICABILITY.—This section does not apply to:
(a) Personal information collected and transmitted that is necessary for the sole purpose of sharing such personal information with a financial service provider to facilitate short term, transactional payment processing for the purchase of products or services.
(b) Personal information collected, used, retained, sold, shared, or disclosed as deidentified personal information or aggregate consumer information.
(c) Compliance with federal, state, or local laws.
(d) Compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

(e) Cooperation with law enforcement agencies concerning conduct or activity that the controller, processor, or third party reasonably and in good faith believes may violate federal, state, or local law.

(f) Exercising legal rights or privileges.

(g) Personal information used or collected by a controller or processor pursuant to a written contract between the controller and processor that complies with the requirements of this section.

(h) Personal information used by a controller or processor to advertise or market products or services that are produced or offered directly by the controller or processor. Such information may not be sold, shared, or disclosed to another person unless otherwise authorized under this section.

(i) Personal information of a person acting in the role of a job applicant, employee, owner, director, officer, contractor, volunteer, or intern of a controller, that is collected by a controller, to the extent the personal information is collected and used solely within the context of the person's role or former role with the controller.

(j) Protected health information for purposes of the federal Health Insurance Portability and Accountability Act of
1996 and related regulations, and patient identifying information for purposes of 42 C.F.R. part 2, established pursuant to 42 U.S.C. s. 290dd-2.

(k) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, or a program or a qualified service program as defined in 42 C.F.R. part 2, to the extent the covered entity, business associate, or program maintains personal information in the same manner as medical information or protected health information as described in paragraph (j), and as long as the covered entity, business associate, or program does not use personal information for targeted advertising with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception under this section.

(l) Identifiable private information collected for purposes of research as defined in 45 C.F.R. s. 164.501 conducted in accordance with the Federal Policy for the Protection of Human Subjects for purposes of 45 C.F.R. part 46, the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, or the Protection for Human Subjects for purposes of 21 C.F.R. parts 50 and 56, or personal information that is used or shared in
research conducted in accordance with one or more of these standards.

(m) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 and related regulations, or patient safety work product for purposes of 42 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21 through 299b-26.

(n) Information that is deidentified in accordance with 45 C.F.R. part 164 and derived from individually identifiable health information as described in the Health Insurance Portability and Accountability Act of 1996, or identifiable personal information, consistent with the Federal Policy for the Protection of Human Subjects or the human subject protection requirements of the United States Food and Drug Administration.

(o) Information used only for public health activities and purposes as described in 45 C.F.R. s. 164.512.

(p) Personal information collected, processed, sold, or disclosed pursuant to the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 and implementing regulations.

(q) Nonpublic personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq., and implementing regulations.

(r) A financial institution as defined in the Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq., to the extent the financial institution maintains personal information in the same
manner as nonpublic personal information as described in paragraph (q), and as long as such financial institution does not use personal information for targeted advertising with third parties and does not sell or share personal information to a third party unless such sale or sharing is covered by an exception under this section.

(s) Personal information collected, processed, sold, or disclosed pursuant to the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. s. 2721 et seq.

(t) Education information covered by the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part 99.

(u) Information collected as part of public or peer-reviewed scientific or statistical research in the public interest and that adheres to all other applicable ethics and privacy laws, if the consumer has provided informed consent. Research with personal information must be subjected by the controller conducting the research to additional security controls that limit access to the research data to only those individuals necessary to carry out the research purpose and subsequently deidentified.

(v) Personal information disclosed for the purpose of responding to an alert of a present risk of harm to a person or property, detecting security incidents, protecting against malicious, deceptive, fraudulent, or illegal activity, or
prosecuting those responsible for that activity.

(w) Personal information that is disclosed when a consumer uses or directs a controller to intentionally disclose information to a third party or uses the controller to intentionally interact with a third party. An intentional interaction occurs when the consumer intends to interact with the third party, by one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

(x) An identifier used for a consumer who has opted out of the sale or sharing of the consumer's personal information for the sole purpose of alerting processors and third parties that the consumer has opted out of the sale or sharing of the consumer's personal information.

(y) Personal information transferred by a controller to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that information is used or shared consistently with this section. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice must be
sufficiently prominent and robust to ensure that consumers can
easily exercise choices consistent with this section.

(2) DEFINITIONS.—As used in this section, the term:
(a) "Aggregate consumer information" means information
that relates to a group or category of consumers, from which the
identity of an individual consumer has been removed and is not
reasonably capable of being directly or indirectly associated or
linked with, any consumer, household, or device. The term does
not include personal information that has been deidentified.
(b) "Biometric information" means an individual's
physiological, biological, or behavioral characteristics,
including an individual's deoxyribonucleic acid (DNA), that can
be used, singly or in combination with each other or with other
identifying data, to establish individual identity. The term
includes, but is not limited to, imagery of the iris, retina,
fingerprint, face, hand, palm, vein patterns, and voice
recordings, from which an identifier template, such as a
faceprint, a minutiae template, or a voiceprint, can be
extracted, and keystroke patterns or rhythms, gait patterns or
rhythms, and sleep, health, or exercise data that contain
identifying information.
(c) "Collect" means to buy, rent, gather, obtain, receive,
or access any personal information pertaining to a consumer by
any means. The term includes, but is not limited to, actively or
passively receiving information from the consumer or by

Page 9 of 31

CODING: Words strucken are deletions; words underlined are additions.
observing the consumer's behavior or actions.

(d) "Consumer" means a natural person who resides in or is domiciled in this state, however identified, including by any unique identifier, who is acting in a personal capacity or household context. The term does not include a natural person acting on behalf of a legal entity in a commercial or employment context.

(e) "Controller" means:

1. A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:
   a. Is organized or operated for the profit or financial benefit of its shareholders or owners;
   b. Does business in this state;
   c. Collects personal information about consumers, or is the entity on behalf of which such information is collected;
   d. Determines the purposes and means of processing personal information about consumers alone or jointly with others; and
   e. Satisfies at least two of the following thresholds:
      (I) Has global annual gross revenues in excess of $50 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.
      (II) Annually buys, receives, sells, or shares the personal information of 50,000 or more consumers, households, or
devices for the purpose of targeted advertising in conjunction with third parties or for a purpose that is not listed under subsection (1).

(III) Derives 50 percent or more of its global annual revenues from selling or sharing personal information about consumers.

2. Any entity that controls or is controlled by a controller. As used in this subparagraph, the term "control" means:

a. Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a controller;

b. Control in any manner over the election of a majority of the directors, or of individuals exercising similar functions; or

c. The power to exercise a controlling influence over the management of a company.

(f) "Deidentified" means information that cannot reasonably be used to infer information about or otherwise be linked to a particular consumer, provided that the controller that possesses the information:

1. Takes reasonable measures to ensure that the information cannot be associated with a specific consumer;

2. Maintains and uses the information in deidentified form and not to attempt to reidentify the information, except that...
the controller may attempt to reidentify the information solely
for the purpose of determining whether its deidentification
processes satisfy the requirements of this paragraph; and

3. Contractually obligates any recipients of the
information to comply with all the provisions of this paragraph
to avoid reidentifying such information.

(g) "Department" means the Department of Legal Affairs.

(h) "Device" means a physical object associated with a
consumer or household capable of directly or indirectly
connecting to the Internet.

(i) "Homepage" means the introductory page of an Internet
website and any Internet webpage where personal information is
collected. In the case of a mobile application, the homepage is
the application's platform page or download page, a link within
the application, such as the "About" or "Information"
application configurations, or settings page, and any other
location that allows consumers to review the notice required by
subsection (7), including, but not limited to, before
downloading the application.

(j) "Household" means a natural person or a group of
people in this state who reside at the same address, share a
common device or the same service provided by a controller, and
are identified by a controller as sharing the same group account
or unique identifier.

(k) "Personal information" means information that is
linked or reasonably linkable to an identified or identifiable consumer or household, including biometric information and unique identifiers to the consumer. The term does not include consumer information that is:

1. Consumer employment contact information, including a position name or title, employment qualifications, emergency contact information, business telephone number, business electronic mail address, employee benefit information, and similar information used solely in an employment context.

2. Deidentified or aggregate consumer information.

3. Publicly and lawfully available information reasonably believed to be made available to the public in a lawful manner and without legal restrictions:
   a. From federal, state, or local government records.
   b. By a widely distributed media source.
   c. By the consumer or by someone to whom the consumer disclosed the information unless the consumer has purposely and effectively restricted the information to a certain audience on a private account.

(l) "Processing" means any operation or set of operations that are performed on personal information or on sets of personal information, whether or not by automated means.

(m) "Processor" means a sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or
financial benefit of its shareholders or other owners, that
processes information on behalf of a controller and to which the
controller discloses a consumer's personal information pursuant
to a written contract, provided that the contract prohibits the
entity receiving the information from retaining, using, or
disclosing the personal information for any purpose other than
for the specific purpose of performing the services specified in
the contract for the controller, or as otherwise permitted by
this section.

(n) "Sell" means to sell, rent, release, disclose,
disseminate, make available, transfer, or otherwise communicate
orally, in writing, or by electronic or other means, a
consumer's personal information by a controller to another
controller or a third party for monetary or other valuable
consideration.

(o) "Share" means to share, rent, release, disclose,
disseminate, make available, transfer, or access a consumer's
personal information for advertising or marketing. The term
includes:

1. Allowing a third party to use or advertise or market to
a consumer based on a consumer's personal information without
disclosure of the personal information to the third party.

2. Monetary transactions, nonmonetary transactions, and
transactions for other valuable consideration between a
controller and a third party for advertising or marketing for
the benefit of a controller.

(p) "Targeted advertising" means marketing to a consumer or displaying an advertisement to a consumer when the advertisement is selected based on personal information used to predict such consumer's preferences or interests.

(q) "Third party" means a person who is not a controller or processor.

(r) "Verifiable consumer request" means a request related to personal information that is made by a consumer, by a parent or guardian on behalf of a consumer who is a minor child, or by a person authorized by the consumer to act on the consumer's behalf in a form that is reasonably and readily accessible to consumers and that the controller can reasonably verify to be the consumer pursuant to rules adopted by the department.

(3) CONSUMER DATA COLLECTION REQUIREMENTS AND RESPONSIBILITIES.—

(a) A controller that collects personal information about consumers shall maintain an up-to-date online privacy policy and make such policy available from its homepage. The online privacy policy must include the following information:

1. Any Florida-specific consumer privacy rights.

2. A list of the types and categories of personal information the controller collects, sells, or shares, or has collected, sold, or shared, about consumers.

3. The consumer's right to request deletion or correction...
of certain personal information.

4. The consumer's right to opt-out of the sale or sharing to third parties.

(b) A controller that collects personal information shall, at or before the point of collection, inform, or direct the processor to inform, consumers of the categories of personal information to be collected and the purposes for which the categories of personal information will be used.

(c) A controller may not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

(d) A controller that collects a consumer's personal information shall implement and maintain reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure. A controller must require any processors and third parties to implement and maintain the same or similar security procedures and practices for personal information.

(e) A controller shall adopt and implement a retention schedule that prohibits the use or retention of personal information 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, after the
expiration or termination of the contract pursuant to which the
information was collected or obtained, or 3 years after the
consumer's last interaction with the controller. This paragraph
does not apply to personal information used or retained for the
following purposes:

1. Detection of security threats or incidents; protection
against malicious, deceptive, fraudulent, unauthorized, or
illegal activity or access; or prosecution of those responsible
for such activity or access.

2. Compliance with a legal obligation, including any
federal retention laws.

3. As reasonably needed for the protection of the
controller's interests related to existing disputes, legal
action, or governmental investigations.

4. Assuring the physical security of persons or property.

(4) CONSUMER RIGHT TO REQUEST COPY OF PERSONAL DATA
COLLECTED, SOLD, OR SHARED.—

(a) A consumer has the right to request that a controller
that collects, sells, or shares personal information about the
consumer to disclose the following to the consumer:

1. The specific pieces of personal information that have
been collected about the consumer.

2. The sources from which the consumer's personal
information was collected.

3. The specific pieces of personal information about the
consumer that were sold or shared.

4. The third parties to which the personal information about the consumer was sold or shared.

5. The categories of personal information about the consumer that were disclosed to a processor.

(b) A controller that collects, sells, or shares personal information about a consumer shall disclose the information specified in paragraph (a) to the consumer upon receipt of a verifiable consumer request.

(c) This subsection does not require a controller to retain, reidentify, or otherwise link any data that, in the ordinary course of business is not maintained in a manner that would be considered personal information.

(d) The controller shall deliver the information required or act on the request in this subsection to a consumer free of charge within 45 days after receiving a verifiable consumer request. The response period may be extended once by 45 additional days when reasonably necessary, provided the controller informs the consumer of any such extension within the initial 45-day response period and the reason for the extension. The information must be delivered in a readily usable format. A controller is not obligated to provide information to the consumer if the consumer or a person authorized to act on the consumer's behalf does not provide verification of identity or verification of authorization to act with the permission of the

Page 18 of 31

CODING: Words **strikethrough** are deletions; words *underlined* are additions.
(e) A controller may provide personal information to a consumer at any time, but is not required to provide personal information to a consumer more than twice in a 12-month period.

(f) This subsection does not apply to personal information relating solely to households.

(5) RIGHT TO HAVE PERSONAL INFORMATION DELETED OR CORRECTED.—

(a) A consumer has the right to request that a controller delete any personal information about the consumer which the controller has collected from the consumer.

(b) A controller that receives a verifiable consumer request to delete the consumer's personal information shall delete the consumer's personal information from its records and direct any processors to delete such information within 90 days of receipt of the verifiable consumer request.

(c) A controller or a processor acting pursuant to its contract with the controller may not be required to comply with a consumer's request to delete the consumer's personal information if it is reasonably necessary for the controller or processor to maintain the consumer's personal information to do any of the following:

1. Complete the transaction for which the personal information was collected.

2. Fulfill the terms of a written warranty or product
recall conducted in accordance with federal law.

3. Provide a good or service requested by the consumer, or reasonably anticipated to be requested within the context of a controller's ongoing business relationship with the consumer, or otherwise perform a contract between the controller and the consumer.

4. Detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity; or prosecute those responsible for that activity.

5. Debug to identify and repair errors that impair existing intended functionality.

6. Engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws when the controller's deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent.

7. Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the controller or that are compatible with the context in which the consumer provided the information.

8. Comply with a legal obligation, including any state or federal retention laws.

9. Reasonably protect the controller's interests against existing disputes, legal action, or governmental investigations.
10. Internally use the consumer's personal information in a lawful manner.

(d) A consumer has the right to make a request to correct inaccurate personal information to a controller that maintains inaccurate personal information about the consumer. A controller that receives a verifiable consumer request to correct inaccurate personal information shall use commercially reasonable efforts to correct the inaccurate personal information as directed by the consumer and direct any processors to correct such information within 90 days after receipt of the verifiable consumer request. If a controller maintains a self-service mechanism to allow a consumer to correct certain personal information, the controller may require the consumer to correct their own personal information through such mechanism.

(6) RIGHT TO OPT-OUT OF THE SALE OR SHARING OF PERSONAL INFORMATION.—

(a) A consumer has the right at any time to direct a controller not to sell or share the consumer's personal information to a third party. This right may be referred to as the right to opt-out.

(b) Notwithstanding paragraph (a), a controller may not sell or share the personal information of a minor consumer if the controller has actual knowledge that the consumer is not 16 years of age or older. However, if a consumer who is between 13
and 16 years of age, or if the parent or guardian of a consumer who is 12 years of age or younger, has affirmatively authorized the sale or sharing of such consumer's personal information, then a controller may sell or share such information in accordance with this section. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age. A controller that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, 15 U.S.C. s. 6501 et seq., shall be deemed compliant with any obligation to obtain parental consent.

(c) A controller that has received direction prohibiting the sale or sharing of the consumer's personal information is prohibited from selling or sharing the consumer's personal information beginning 48 hours after receipt of such direction, unless the consumer subsequently provides express authorization for the sale or sharing of the consumer's personal information.

(7) FORM TO OPT-OUT OF SALE OR SHARING OF PERSONAL INFORMATION.—

(a) A controller shall:

1. In a form that is reasonably accessible to consumers, provide a clear and conspicuous link on the controller's Internet homepage, entitled "Do Not Sell or Share My Personal Information," to an Internet webpage that enables a consumer, or a person authorized by the consumer, to opt-out of the sale or
sharing of the consumer's personal information. A controller may
not require a consumer to create an account in order to direct
the controller not to sell the consumer's personal information.
A controller may accept a request to opt-out received through a
user-enabled global privacy control, such as a browser plug-in
or privacy setting, device setting, or other mechanism, which
communicates or signals the consumer's choice to opt out.

2. For consumers who opted-out of the sale or sharing of
t heir personal information, respect the consumer's decision to
opt-out for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's
personal information.

3. Use any personal information collected from the consumer in connection with the submission of the consumer's opt-out request solely for the purposes of complying with the opt-out request.

(b) A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information on the consumer's behalf pursuant to rules adopted by the department.

(8) ACTIONS RELATED TO CONSUMERS WHO EXERCISE PRIVACY RIGHTS.—

(a) A controller may charge a consumer who exercised any
of the consumer's rights under this section a different price or
rate, or provide a different level or quality of goods or
services to the consumer, only if that difference is reasonably related to the value provided to the controller by the consumer's data or is related to a consumer's voluntary participation in a financial incentive program, including a bona fide loyalty, rewards, premium features, discounts, or club card program offered by the controller.

(b) A controller may offer financial incentives, including payments to consumers as compensation, for the collection, sharing, sale, or deletion of personal information if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program. The consent may be revoked by the consumer at any time.

(c) A controller may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(9) CONTRACTS AND ROLES.—
   (a) Any contract or agreement between a controller and a processor must:
       1. Prohibit the processor from selling, sharing, retaining, using, or disclosing the personal information other than for the purposes specified in the contract or agreement with the controller;
       2. Govern the processor's personal information processing procedures with respect to processing performed on behalf of the controller, including processing instructions, the nature and purpose of processing, the type of information subject to
processing, the duration of processing, and the rights and
obligations of both the controller and processor;

3. Require the processor to return or delete all personal
information under the contract to the controller as requested by
the controller at the end of the provision of services, unless
retention of the information is required by law; and

4. Upon request of the controller, require the processor
to make available to the controller all information in its
possession under the contract or agreement.

(b) Determining whether a person is acting as a controller
or processor with respect to a specific processing of data is a
fact-based determination that depends upon the context in which
personal information is to be processed. The contract between a
controller and processor must reflect their respective roles and
relationships related to handling personal information. A
processor that continues to adhere to a controller's
instructions with respect to a specific processing of personal
information remains a processor.

(c) A third party may not sell or share personal
information about a consumer that has been sold or shared to the
third party by a controller unless the consumer has received
explicit notice from the third party and is provided an
opportunity to opt-out by the third party.

(d) A processor or third party must require any
subcontractor to meet the same obligations of such processor or
third party with respect to personal information.

(e) A processor or third party or any subcontractor thereof who violates any of the restrictions imposed upon it under this section is liable or responsible for any failure to comply with this section.

(f) Any provision of a contract or agreement of any kind that waives or limits in any way a consumer's rights under this section, including, but not limited to, any right to a remedy or means of enforcement, is deemed contrary to public policy and is void and unenforceable. This section does not prevent a consumer from declining to request information from a controller, declining to opt-out of a controller's sale or sharing of the consumer's personal information, or authorizing a controller to sell or share the consumer's personal information after previously opting out.

(10) CIVIL ACTIONS; PRIVATE RIGHT OF ACTION.—

(a) A Florida consumer may only bring a civil action against a controller, processor, or person pursuant to this section for the following:

1. Failure to delete or correct a consumer's personal information pursuant to this section after receiving a verifiable consumer request or directions to delete or correct from a controller unless the controller, processor, or person qualifies for an exception to the requirements to delete or correct under this section.
2. Continuing to sell or share a consumer's personal information after the consumer chooses to opt-out pursuant to this section.

3. Selling or sharing the personal information of a consumer age 16 or younger without obtaining consent as required by this section.

(b) A court may grant the following relief to a consumer:

1. Damages in an amount not less than $100 and not greater than $750 per consumer per incident or actual damages, whichever is greater.

2. Injunctive or declaratory relief.

(c) Upon prevailing, the consumer shall recover reasonable attorney fees and costs.

(d) Any action under this subsection may only be brought by or on behalf of a Florida consumer.

(e) Liability for a tort, contract claim, or consumer protection claim which is unrelated to an action brought under subsection (10) or subsection (11) does not arise solely from the failure of a controller, processor, or person to comply with this section and evidence of such may only be used as the basis to prove a cause of action under this subsection.

(11) ENFORCEMENT AND IMPLEMENTATION BY THE DEPARTMENT.—

(a) Any violation of this section is an unfair and deceptive trade practice actionable under part II of chapter 501 solely by the department against a controller, processor, or
person. If the department has reason to believe that any controller, processor, or person is in violation of this section, the department, as the enforcement authority, may bring an action against such controller, processor, or person for an unfair or deceptive act or practice. For the purpose of bringing an action pursuant to this section, ss. 501.211 and 501.212 do not apply. Civil penalties may be tripled if the violation:

1. Involves a consumer who the controller, processor, or person has actual knowledge is 16 years of age or younger; or
2. Is based on paragraph (10)(a).

(b) After the department has notified a controller, processor, or person in writing of an alleged violation, the department may in its discretion grant a 45-day period to cure the alleged violation. The 45-day cure period does not apply to a violation of subparagraph (10)(a)1. The department may consider the number and frequency of violations, the substantial likelihood of injury to the public, and the safety of persons or property when determining whether to grant 45 days to cure and the issuance of a letter of guidance. If the violation is cured to the satisfaction of the department and proof of such cure is provided to the department, the department in its discretion may issue a letter of guidance. If the controller, processor, or person fails to cure the violation within 45 days, the department may bring an action against the controller, processor, or person for the alleged violation.
(c) Any action brought by the department may only be brought by or on behalf of a Florida consumer.

(d) By February 1 of each year, the department shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing any actions taken by the department to enforce this section. The report shall include statistics and relevant information detailing:

1. The number of complaints received;
2. The number and type of enforcement actions taken and the outcomes of such actions;
3. The number of complaints resolved without the need for litigation; and
4. The status of the development and implementation of rules to implement this section.

(e) The department may adopt rules to implement this section, including standards for verifiable consumer requests, enforcement, data security, and authorized persons who may act on a consumer's behalf.

(12) JURISDICTION.—For purposes of bringing an action in accordance with subsections (10) and (11), any person who meets the definition of controller as defined in this section that collects, shares, or sells the personal information of Florida consumers, is considered to be both engaged in substantial and not isolated activities within this state and operating, conducting, engaging in, or carrying on a business, and doing
business in this state, and is therefore subject to the
jurisdiction of the courts of this state.

(13) PREEMPTION.—This section is a matter of statewide
concern and supersedes all rules, regulations, codes,
ordinances, and other laws adopted by a city, county, city and
county, municipality, or local agency regarding the collection,
processing, sharing, or sale of consumer personal information by
a controller or processor. The regulation of the collection,
processing, sharing, or sale of consumer personal information by
a controller or processor is preempted to the state.

Section 2. Paragraph (g) of subsection (1) of section
501.171, Florida Statutes, is amended to read:

501.171 Security of confidential personal information.—
(1) DEFINITIONS.—As used in this section, the term:
(g)1. "Personal information" means either of the
following:

a. 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 license or identification card number,
passport number, military identification number, or other
similar number issued on a government document used to verify
identity;
(III) 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.
   (VI) An individual's biometric information as defined in
s. 501.173(2).
   b. A user name or e-mail address, in combination with a
password or security question and answer that would permit
access to an online account.
2. The term does not include information about an
individual that has been made publicly available by a federal,
state, or local governmental entity. The term also does not
include information that is encrypted, secured, or modified by
any other method or technology that removes elements that
personally identify an individual or that otherwise renders the
information unusable.
Section 3. This act shall take effect July 1, 2023.
By Senator Bradley

A bill to be entitled
An act relating to consumer data privacy; creating s.
501.172, F.S.; providing a short title; creating s.
501.173, F.S.; providing a purpose; creating s.
501.174, F.S.; defining terms; creating s. 501.1745,
F.S.; requiring controllers that collect consumer
personal information to provide certain information to
the consumer; requiring such collection, use, and
retention of such information to meet certain
requirements; requiring controllers to implement
reasonable security procedures and practices;
prohibiting controllers from processing certain
sensitive consumer data under certain circumstances;
creating s. 501.175, F.S.; providing that consumers
have the right to opt out of the sale and processing
of their personal information by controllers;
providing requirements for a controller to comply with
such a request under certain circumstances;
prohibiting controllers from selling the personal
information of consumers younger than a specified age
without express authorization from the consumer or the
consumer’s parent or guardian under certain
circumstances; providing that businesses that
willfully disregard a consumer’s age are deemed to
have actual knowledge of the consumer’s age; providing
requirements for controllers to comply with a
consumer’s right to opt out; providing exceptions;
providing that consumers have the right to submit a
verified request for the deletion or correction of
their personal information; providing construction;
providing that consumers may authorize other persons
to opt out of the sale of the consumer’s personal
information on the consumer’s behalf; requiring
controllers to establish designated request addresses;
providing requirements for controllers to comply with
verified consumer requests; providing notice
requirements; authorizing businesses to charge
consumers a reasonable fee for manifestly unfounded or
excessive requests, or to refuse to complete a request
under certain circumstances; providing that
controllers and processors are not liable for certain
actions; providing that third-party controllers or
processors are liable for violating the act or the
terms of certain contractual agreements, thereby
resulting in a violation; providing that a consumer’s
rights and the obligations of a controller may not
adversely affect the rights and freedoms of other
consumers; creating s. 501.176, F.S.; providing
applicability; providing exceptions; defining the
terms “vehicle information” and “ownership
information”; creating s. 501.177, F.S.; providing
applicability; specifying violations that are
enforceable by the Department of Legal Affairs under
the Florida Deceptive and Unfair Trade Practices Act;
authorizing the department to grant controllers and
processors an opportunity to cure violations when
given notice by the department; providing civil
remedies and penalties for violations; authorizing
increased civil penalties for certain violations; requiring the department, in conjunction and consultation with the director of the Consumer Data Privacy Unit, to submit a report to the Legislature by a specified date; providing requirements for the report; authorizing the department to adopt rules; providing for jurisdiction; preempting the regulation of the collection, processing, or sale of consumers’ personal information by a controller or processor to the state; amending s. 16.53, F.S.; revising the purposes for which the Legal Affairs Revolving Trust Fund may be used to include enforcement of the Florida Privacy Protection Act by the Attorney General; requiring that attorney fees and costs recovered by the Attorney General for certain actions be deposited in the fund; creating s. 16.581, F.S.; creating the Consumer Data Privacy Unit within the department; providing for a director of the unit; providing the duties of the unit; authorizing the unit to take certain actions; authorizing the unit to recover reasonable attorney fees and costs and penalties in accordance with certain provisions; requiring such moneys to be deposited in the Legal Affairs Revolving Trust Fund; requiring other moneys recovered by the Attorney General for penalties to be deposited into the General Revenue Fund; providing an effective date.

Be It Enacted by the Legislature of the State of Florida:
Section 1. Section 501.172, Florida Statutes, is created to read:

501.172 Short title.—This act, consisting of ss. 501.172-501.177, may be cited as the “Florida Privacy Protection Act.”

Section 2. Section 501.173, Florida Statutes, is created to read:

501.173 Purpose.—This act recognizes that privacy is an important right, and consumers in this state should have the ability to share their personal information as they wish, in a way that is safe and that they understand and control.

Section 3. Section 501.174, Florida Statutes, is created to read:

501.174 Definitions.—As used in ss. 501.172-501.177, unless the context otherwise requires, the term:

(1) “Affiliate” means a legal entity that controls, is controlled by, or is under common control with another legal entity or shares common branding with another legal entity. For the purposes of this subsection, the term “control” or “controlled” means the ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise controlling influence over the management of a company.

(2) “Aggregate consumer information” means information that relates to a group or category of consumers from which individual consumer identities have been removed and which is not linked or reasonably linkable to any consumer, including through a device. The term does not include one or more
(3) "Authenticate" means verifying through reasonable means that the consumer entitled to exercise his or her consumer rights under this act is the same consumer exercising such consumer rights with respect to the personal information at issue.

(4) "Biometric information" means personal information generated by automatic measurements of an individual’s physiological, behavioral, or biological characteristics, including an individual’s DNA, which identifies an individual. The term does not include a physical or digital photograph; a video or audio recording or data generated therefrom; or information collected, used, or stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996.

(5) "Business purpose" means the use of personal information for the controller’s operational, administrative, security, or other purposes allowed for under this act, or for any notice-given and consumer-approved purposes or for the processor’s operational purposes, provided that the use of the personal information is consistent with the requirements of this act.

(6) "Child" means a natural person younger than 13 years of age.

(7) "Collects," "collected," or "collection" means buying, renting, gathering, obtaining, receiving, or accessing by any means any personal information pertaining to a consumer, either actively or passively or by observing the consumer’s behavior.

(8) "Consumer" means a natural person who resides in this state.
state to the extent he or she is acting in an individual or household context. The term does not include any other natural person who is a nonresident or a natural person acting in a commercial or employment context.

(9) “Controller” means a sole proprietorship, a partnership, a limited liability company, a corporation, or an association or any other legal entity that meets the following requirements:

(a) Is organized or operated for the profit or financial benefit of its shareholders or owners;

(b) Does business in this state or provides products or services targeted to the residents of this state;

(c) Determines the purposes and means of processing personal information about consumers, alone or jointly with others; and

(d) Satisfies either of the following thresholds:

1. During a calendar year, controls the processing of the personal information of 100,000 or more consumers who are not covered by an exception under this act; or

2. Controls or processes the personal information of at least 25,000 consumers who are not covered by an exception under this act and derives 50 percent or more of its global annual revenues from selling personal information about consumers.

(10) “De-identified” means information that cannot reasonably identify or be linked directly to a particular consumer, or a device linked to such consumer, if the controller or a processor that possesses such information on behalf of the controller:

(a) Has taken reasonable measures to ensure that the
information cannot be associated with an individual consumer; 
(b) Commits to maintain and use the information in a de-
identified fashion without attempting to reidentify the 
information; and
(c) Contractually prohibits downstream recipients from 
attempting to reidentify the information.
(11) “Designated request address” means an e-mail address, 
a toll-free telephone number, or a website established by a 
controller through which a consumer may submit a verified 
request to the controller.
(12) “Intentional interaction” or “intentionally 
interacting” means that the consumer intends to interact with or 
disclose personal information to a person through one or more 
deliberate interactions, including visiting the person’s website 
or purchasing a good or service from the person. The term does 
not include hovering over, muting, pausing, or closing a given 
piece of content.
(13) “Non-targeted advertising” means:
(a) Advertising based solely on a consumer’s activities 
within a controller’s own, or its affiliates’, websites or 
online applications;
(b) Advertisements based on the context of a consumer’s 
current search query, visit to a website, or online application;
(c) Advertisements directed to a consumer in response to 
the consumer’s request for information or feedback; or
(d) Processing personal information solely for measuring or 
reporting advertising performance, reach, or frequency.
(14) “Personal information” means:
(a) Information that identifies or is linked or reasonably
linkable to an identified or identifiable consumer.

(b) The term does not include:

1. Information about a consumer that is lawfully made available through federal, state, or local governmental records;

2. Information that a controller has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media unless the consumer has restricted the information to a specific audience; or

3. Consumer information that is de-identified or aggregate consumer information.

(15) “Precise geolocation data” means information from technology, such as global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of a natural person with precision and accuracy within a radius of 1,750 feet. The term does not include the information generated by the transmission of communications or any information generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

(16) “Process” or “processing” means any operation or set of operations performed on personal information or on sets of personal information, regardless of whether by automated means.

(17) “Processor” means a natural or legal entity that processes personal data on behalf of, and at the direction of, a controller.

(18) “Profiling” means any form of automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable natural person’s economic situation, health, personal
preferences, interests, reliability, behavior, location, or movements. The term does not include processing personal information solely for the purpose of measuring or reporting advertising performance, reach, or frequency.

(19) “Pseudonymous information” means personal information that cannot be attributed to a specific natural person without the use of additional information, which must be kept separate at all times and must be subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to or combined with other personal data that may enable attribution to an identified or identifiable natural person.

(20) “Security and integrity” means the ability of a:

(a) Network or information system, device, website, or online application to detect security incidents that compromise the availability, authenticity, integrity, and confidentiality of stored or transmitted personal information;

(b) Controller to detect security incidents; resist malicious, deceptive, fraudulent, or illegal actions; and help prosecute those responsible for such actions; and

(c) Controller to ensure the physical safety of natural persons.

(21) “Sell” means to transfer or make available a consumer’s personal information by a controller to a third party in exchange for monetary or other valuable consideration, including nonmonetary transactions and agreements for other valuable consideration between a controller and a third party for the benefit of a controller. The term does not include any of the following:
(a) The disclosure, for a business purpose, of a consumer’s personal information to a processor that processes the information for the controller.

(b) The disclosure by a controller for the purpose of providing a product or service requested or approved by a consumer, or the parent of a child, of the consumer’s personal information to a third-party entity.

(c) The disclosure or transfer of personal information to an affiliate of the controller.

(d) The disclosure of personal information for purposes of nontargeted advertising.

(e) The disclosure or transfer of personal information to a third party as an asset that is part of a proposed or actual merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller’s assets.

(f) The controller disclosing personal information to a law enforcement or other emergency processor for the purposes of providing emergency assistance to the consumer.

(22) “Sensitive data” means a category of personal information that includes any of the following:

(a) Racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.

(b) Biometric information, including genetic information, processed for the purpose of uniquely identifying a natural person.

(c) Personal information collected from a known child.

(d) Precise geolocation data.
“Targeted advertising” means displaying an advertisement to a consumer when the advertisement is selected based on personal information obtained from the consumer’s activities over time and across nonaffiliated websites or online applications to predict such consumer’s preferences or interests. The term does not include any of the following:

(a) Non-targeted advertising.
(b) Advertisements based on the context of a consumer’s current search query or visit to a website.
(c) Advertising directed to a consumer in response to the consumer’s request for information or feedback.
(d) Processing personal data solely for the purpose of measuring or reporting advertising performance, reach, or frequency.

“Third party” means a person who is not any of the following:

(a) The controller with which the consumer intentionally interacts and which collects personal information from the consumer as part of the consumer’s interaction with the controller.
(b) A processor that processes personal information on behalf of and at the direction of the controller.
(c) An affiliate of the controller.

“Verified request” means a request submitted by a consumer or by a consumer on behalf of the consumer’s minor child for which the controller has reasonably verified the authenticity of the request. The term includes a request made through an established account using the controller’s established security features to access the account through
communication features offered to consumers. The term does not include a request in which the consumer or a person authorized to act on the consumer’s behalf does not provide verification of identify or verification of authorization to act with the permission of the consumer, and the controller is not required to provide information for such a request.

Section 4. Section 501.1745, Florida Statutes, is created to read:

501.1745 General duties of controllers that collect personal information.—

(1) A controller that controls the collection of a consumer’s personal information that will be used for any purpose other than a business purpose, at or before the point of collection, shall inform consumers of the purposes for which personal information is collected or used and whether that information is sold. A controller may not collect additional categories of personal information, or use collected personal information for additional purposes that are incompatible with the disclosed purpose for which the personal information was collected, without providing the consumer with notice consistent with this section. A controller that collects personal information about, but not directly from, consumers may provide the required information on its Internet home page or in its online privacy policy.

(2) A controller’s collection, use, and retention of a consumer’s personal information must be reasonably necessary to achieve the purposes for which the personal information was collected or processed. Such information may not be further processed in a manner that is incompatible with those purposes.
without notice to the consumer or be transferred or made available to a third party in a manner inconsistent with the requirements of this act.

(3) A controller that collects a consumer’s personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure.

(4) A controller that collects a consumer’s personal information and discloses it to a processor shall enter into a contractual agreement with such processor which obligates the processor to comply with applicable obligations under this act and which prohibits downstream recipients from selling personal information or retaining, using, or disclosing the personal information. If a processor engages any other person to assist it in processing personal information for a business purpose on behalf of the controller, or if any other person engaged by the processor engages another person to assist in processing personal information for that business purpose, the processor or person must notify the controller of that engagement and the processor must prohibit downstream recipients from selling the personal information or retaining, using, or disclosing the personal information.

(5) A controller may not process sensitive data concerning a consumer without obtaining the consumer’s consent or, in the case of the processing of sensitive data obtained from a known child, without processing such data for the purpose of delivering a product or service requested by the parent of such child, or in accordance with the federal Children’s Online
Privacy Protection Act, 15 U.S.C. s. 6501 et seq. and regulations interpreting this act.

(6) The determination as to whether a person is acting as a controller or processor with respect to a specific activity is a fact-based determination that depends upon the context in which personal information is processed. A processor that continues to adhere to a controller’s instructions with respect to a specific processing of personal information remains a processor.

Section 5. Section 501.175, Florida Statutes, is created to read:

501.175 Use of personal information; third parties; other rights.—

(1)(a) A consumer has the right at any time to direct a controller that sells personal information about the consumer not to sell the consumer’s personal information. This right may be referred to as the right to opt out of the sale.

(b) A consumer has the right at any time to opt out of the processing of the consumer’s personal information for purposes of targeted advertising or profiling. A controller shall provide a clear and conspicuous link on the controller’s Internet home page, titled “Do Not Advertise To Me,” to a web page that enables a consumer to opt out of targeted advertising or profiling. However, this paragraph may not be construed to prohibit the controller that collected the consumer’s personal information from:

1. Offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has opted out of targeted advertising, profiling, or the sale of his or her
2. Offering a loyalty, reward, premium feature, discount, or club card program.

(c) A controller that charges or offers a different price, rate, level, quality, or selection of goods or services to a consumer who has opted out of targeted advertising, profiling, or the sale of his or her personal information, or that offers goods or services for no fee, shall ensure that such charge or offer is not unjust, unreasonable, coercive, or usurious.

(2) A controller that sells consumers’ personal information shall provide notice to consumers that the information may be sold and that consumers have the right to opt out of the sale of their personal information.

(3) A controller that sells consumers’ personal information and that has received direction from a consumer not to sell the consumer’s personal information or, in the case of a minor consumer’s personal information, has not received consent to sell the minor consumer’s personal information, is prohibited from selling the consumer’s personal information after the controller receives the consumer’s direction, unless the consumer subsequently provides express authorization for the sale of the consumer’s personal information. A controller that is able to authenticate the consumer by the consumer logging in or any other means, or that is otherwise reasonably able to authenticate the consumer’s request must comply with the consumer’s request to opt out. The controller may not require the consumer to declare privacy preferences every time the consumer visits the controller’s website or uses the controller’s online services.
(4)(a) A controller may not sell the personal information collected from consumers that the controller has actual knowledge are 16 years of age or younger, unless:

1. The consumer, in the case of consumers who are 13 years of age up to 16 years of age, has affirmatively authorized the sale of the consumer’s personal information; or

2. The consumer’s parent or guardian, in the case of consumers who are younger than 13 years of age, has affirmatively authorized such sale.

(b) This right may be referred to as the right to opt in.

(c) A business that willfully disregards the consumer’s age is deemed to have actual knowledge of the consumer’s age.

(d) A controller that complies with the verifiable parental consent requirements of the Children’s Online Privacy Protection Act, 15 U.S.C. s. 6501 et seq., and accompanying regulations, or is providing a product or service requested by a parent or guardian, is deemed compliant with any obligation to obtain parental consent.

(5) A controller required to comply with this section shall:

(a) Provide a clear and conspicuous link on the controller’s Internet home page, titled “Do Not Sell My Personal Information,” to a web page that enables a consumer to opt out of the sale of the consumer’s personal information. A business may not require a consumer to create an account in order to direct the business not to sell the consumer’s information.

(b) Ensure that all individuals responsible for handling consumer inquiries about the controller’s privacy practices or the controller’s compliance with this section are informed of
all requirements of this section and how to direct consumers to exercise their rights.

(c) For consumers who exercise their right to opt out of the sale of their personal information, refrain from selling personal information the controller collected about the consumer as soon as reasonably possible but no longer than 10 business days after receiving the request to opt out.

(d) Use any personal information collected from the consumer in connection with the submission of the consumer’s opt-out request solely for the purposes of complying with the opt-out request.

(e) For consumers who have opted out of the sale of their personal information, respect the consumer’s decision to opt out for at least 12 months before requesting that the consumer authorize the sale of the consumer’s personal information.

(f) Ensure that consumers have the right to submit a verified request for certain information from a controller, including the categories of sources from which the consumer’s personal information was collected, the specific items of personal information it has collected about the consumer, and the categories of any third parties to whom the personal information was sold.

(6) Consumers have the right to submit a verified request that personal information that has been collected from the consumer be deleted. Consumers have the right to submit a verified request for correction of their personal information held by a controller if that information is inaccurate, taking into account the nature of the personal information and the purpose for processing the consumer’s personal information.
(7) A controller, or a processor acting pursuant to its contract with the controller or another processor, is not required to comply with a consumer’s verified request to delete the consumer’s personal information if it is necessary for the controller or processor to maintain the consumer’s personal information in order to do any of the following:

(a) Complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or otherwise perform a contract between the business and the consumer.

(b) Help to ensure security and integrity to the extent that the use of the consumer’s personal information is reasonably necessary and proportionate for those purposes.

(c) Debug to identify and repair errors that impair existing intended functionality.

(d) Exercise free speech, ensure the right of another consumer to exercise that consumer’s right of free speech, or exercise another right provided for by law.

(e) Engage in public or peer-reviewed scientific, historical, or statistical research that conforms or adheres to all other applicable ethics and privacy laws, when the business’ deletion of the information is likely to render impossible or seriously impair the ability to complete such research, if the consumer has provided informed consent.

(f) Comply with a legal obligation.

(8) This section may not be construed to require a controller to comply by reidentifying or otherwise linking
information that is not maintained in a manner that would be considered personal information; retaining any personal information about a consumer if, in the ordinary course of business, that information would not be retained; maintaining information in identifiable, linkable, or associable form; or collecting, obtaining, retaining, or accessing any data or technology in order to be capable of linking or associating a verifiable consumer request with personal information.

(9) A consumer may authorize another person to opt out of the sale of the consumer’s personal information. A controller shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer’s behalf, including a request received through a user-enabled global privacy control, such as a browser plug-in or privacy setting, device setting, or other mechanism, which communicates or signals the consumer’s choice to opt out, and may not require a consumer to make a verified request to opt out of the sale of his or her information.

(10) Each controller shall establish a designated request address through which a consumer may submit a request to exercise his or her rights under this act.

(11)(a) A controller that receives a verified request:

1. For a consumer’s personal information shall disclose to the consumer any personal information about the consumer which it has collected since January 1, 2023, directly or indirectly, including such information obtained through or by a processor.

2. To correct a consumer’s inaccurate personal information shall correct the inaccurate personal information, taking into account the nature of the personal information and the purpose
for processing the consumer’s personal information.

3. To delete a consumer’s personal information shall delete such personal information collected from the consumer.

(b) A processor is not required to personally comply with a verified request received directly from a consumer, but the processor must notify a controller of such a request within 10 days after receiving the request. The time period required for a controller to comply with a verified request as provided in paragraph (d) commences beginning from the time the processor notifies the controller of the verified request. A processor shall provide reasonable assistance to a controller with which it has a contractual relationship with respect to the controller’s response to a verifiable consumer request, including, but not limited to, by providing to the controller the consumer’s personal information in the processor’s possession which the processor obtained as a result of providing services to the controller.

(c) At the direction of the controller, a processor shall correct inaccurate personal information or delete personal information, or enable the controller to do the same.

(d) A controller shall comply with a verified request submitted by a consumer to access, correct, or delete personal information within 45 days after the date the request is submitted. A controller may extend such period by up to 45 days if the controller, in good faith, determines that such an extension is reasonably necessary. A controller that extends the period shall notify the consumer of the necessity of an extension.

(e) A consumer’s rights under this subsection do not apply
to pseudonymous information in cases in which the controller is able to demonstrate that all information necessary to identify the consumer is kept separate at all times and is subject to effective technical and organizational controls that prevent the controller from accessing or combining such information.

(12) A controller shall comply with a consumer’s previous expressed decision to opt out of the sale of his or her personal information without requiring the consumer to take any additional action if the controller is able to identify the consumer through a login protocol or any other process the controller uses to identify consumers and the consumer has previously exercised his or her right to opt out of the sale of his or her personal information.

(13) A controller shall make available, in a manner reasonably accessible to consumers whose personal information the controller collects through its website or online service, a notice that does all of the following:

(a) Identifies the categories of personal information that the controller collects through its website or online service about consumers who use or visit the website or online service and the categories of third parties to whom the controller may disclose such personal information.

(b) Provides a description of the process, if applicable, for a consumer who uses or visits the website or online service to review and request changes to any of his or her personal information collected from the consumer through the website or online service.

(c) Describes the process by which the controller notifies consumers who use or visit the website or online service of
(d) Discloses whether a third party may collect personal information about a consumer’s online activities over time and across different websites or online services when the consumer uses the controller’s website or online service.

(e) States the effective date of the notice.

(14) If a request from a consumer is manifestly unfounded or excessive, in particular because of the request’s repetitive character, a controller may either charge a reasonable fee, taking into account the administrative costs of providing the information or communication or taking the action requested, or refuse to act on the request and notify the consumer of the reason for refusing the request. The controller bears the burden of demonstrating that any verified consumer request is manifestly unfounded or excessive.

(15) A controller that discloses personal information to a processor is not liable under this act if the processor receiving the personal information uses it in violation of the restrictions set forth in the act, provided that, at the time of disclosing the personal information, the controller does not have actual knowledge or reason to believe that the processor intends to commit such a violation. A processor is likewise not liable under this act for the obligations of a controller for which it processes personal information as set forth in this act.

(16) A controller or processor that discloses personal information to a third-party controller or processor in compliance with the requirements of this act is not in violation of this chapter if the third-party controller or processor that
receives and processes such personal information is in violation of this act, provided that, at the time of disclosing the personal information, the disclosing controller or processor did not have actual knowledge that the recipient intended to commit a violation. A third-party controller or processor that violates this act, or violates the terms of a contractual agreement with a controller or processor which results in a violation of this act, is deemed to have violated the requirements of this act and is subject to the enforcement actions otherwise provided against a controller pursuant to s. 501.177. A third-party controller or processor receiving personal information from a controller or processor in compliance with the requirements of this act is not in violation of this act for noncompliance of the controller or processor from which it receives such personal data.

(17) The rights afforded to consumers and the obligations imposed on a controller in this act may not adversely affect the rights and freedoms of other consumers. Notwithstanding subsection (7), a verified request for specific items of personal information, to delete a consumer’s personal information, or to correct inaccurate personal information does not extend to personal information about the consumer which belongs to, or which the controller maintains on behalf of, another natural person.

Section 6. Section 501.176, Florida Statutes, is created to read:

501.176 Applicability; exclusions.—
(1) The obligations imposed on a controller or processor by this act do not restrict a controller’s or processor’s ability to do any of the following:
5-01351-22

(a) Comply with federal, state, or local laws, rules, or regulations.

(b) Comply with a civil, criminal, or regulatory inquiry or an investigation, a subpoena, or a summons by federal, state, local, or other governmental authorities.

(c) Cooperate with law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal, state, or local laws, rules, or regulations.

(d) Exercise, investigate, establish, prepare for, or defend legal claims.

(e) Collect, use, retain, sell, or disclose consumer personal information to:

1. Conduct internal research to develop, improve, or repair products, services, or technology;

2. Effectuate a product recall or provide a warranty for products or services;

3. Identify or repair technical errors that impair existing or intended functionality;

4. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer’s existing relationship with the controller or that are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or a parent of a child, or the performance of a contract to which the consumer is a party;

5. Provide a product or service specifically requested by a consumer or a parent of a child; perform a contract to which the consumer or parent is a party, including fulfilling the terms of
5-01351-22

a written warranty; or take steps at the request of the consumer
before entering into a contract;

6. Take steps to protect an interest that is essential for
the life or physical safety of the consumer or of another
natural person, and where the processing cannot be manifestly
based on another legal basis;

7. Prevent, detect, protect against, or respond to security
incidents, identity theft, fraud, harassment, malicious or
deceptive activities, or any illegal activity, and prosecute
those responsible for that activity;

8. Preserve the integrity or security of information
technology systems;

9. Investigate, report, or prosecute those responsible for
any illegal, malicious, harmful, deceptive, or otherwise harmful
activities;

10. Engage in public or peer-reviewed scientific or
statistical research in the public interest that adheres to all
other applicable ethics and privacy laws and, if applicable, is
approved, monitored, and governed by an institutional review
board, or similar independent oversight entity that determines
if the information is likely to provide substantial benefits
that do not exclusively accrue to the controller, if the
expected benefits of the research outweigh the privacy risks,
and if the controller has implemented reasonable safeguards to
mitigate privacy risks associated with research, including any
risks associated with reidentification; or

11. Assist another controller, processor, or third party
with any of the obligations under this subsection.

(2) This act does not apply to any of the following:
(a) A controller that collects, processes, or discloses the personal information of its employees, owners, directors, officers, beneficiaries, job applicants, interns, or volunteers, so long as the controller is collecting or disclosing such information only to the extent reasonable and necessary within the scope of the role the controller has in relation to each class of listed individuals. For purposes of this section the term “personal information” includes employment benefit information.

(b) Personal information that is part of a written or verbal communication or a transaction between the controller or processor and the consumer, when the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, nonprofit, or government agency and whose communications or transaction with the business occur solely within the context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, nonprofit, or government agency.

(c) A business, service provider, or third party that collects the personal information of an individual:

1. Who applies to, is or was previously employed by, or acts as an agent of the business, service provider, or third party, to the extent that the personal information is collected and used in a manner related to or arising from the individual’s employment status; or

2. To administer benefits for another individual and the personal information is used to administer those benefits.
(d) A business that enters into a contract with an independent contractor and collects or discloses personal information about the contractor reasonably necessary to either enter into or to fulfill the contract when the contracted services would not defeat the purposes of this act.

(e) Protected health information for purposes of the federal Health Insurance Portability and Accountability Act of 1996 and related regulations, and patient identifying information for purposes of 42 C.F.R. part 2, established pursuant to 42 U.S.C. s. 290dd-2.

(f) A covered entity or business associate governed by the privacy, security, and breach notification rules issued by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, or a program or a qualified service program defined in 42 C.F.R. part 2, to the extent that the covered entity, business associate, or program maintains personal information in the same manner as medical information or protected health information as described in paragraph (e).

(g) Identifiable private information collected for purposes of research as defined in 45 C.F.R. s. 164.501 which is conducted in accordance with the Federal Policy for the Protection of Human Subjects for purposes of 45 C.F.R. part 46, the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use, or the Protection for Human Subjects for purposes of 21 C.F.R. parts 50 and 56; or personal information used or shared in research conducted in accordance with one or more of these standards, or another applicable protocol.
(h) Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986 and related regulations, or patient safety work product for purposes of 42 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21 through 299b-26.

(i) Information de-identified in accordance with 45 C.F.R. part 164 and derived from individually identifiable health information, as described in the federal Health Insurance Portability and Accountability Act of 1996, or identifiable personal information, consistent with the Federal Policy for the Protection of Human Subjects or the human subject protection requirements of the United States Food and Drug Administration or the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use.

(j) Information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects pursuant to good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or pursuant to human subject protection requirements of the United States Food and Drug Administration, or another protocol.

(k) Personal information collected, processed, sold, or disclosed pursuant to the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 et seq.

(l) Personal information collected, processed, sold, or disclosed pursuant to, or a financial institution to the extent regulated by, the federal Gramm-Leach-Bliley Act, 15 U.S.C. s. 6801 et seq. and implementing regulations.
(m) Personal information collected, processed, sold, or disclosed pursuant to the Farm Credit Act of 1971, as amended in 12 U.S.C. s. 2001-2279cc and implementing regulations.

(n) Personal information collected, processed, sold, or disclosed pursuant to the federal Driver’s Privacy Protection Act of 1994, 18 U.S.C. s. 2721 et seq.


(p) Personal information collected, processed, sold, or disclosed in relation to price, route, or service as those terms are used in the federal Airline Deregulation Act, 49 U.S.C. s. 40101 et seq., by entities subject to the federal Airline Deregulation Act, to the extent this act is preempted by s. 41713 of the federal Airline Deregulation Act.

(q) Vehicle information or ownership information retained or shared between a new motor vehicle dealer, a distributor, or the vehicle’s manufacturer if the vehicle or ownership information is shared for the purpose of effectuating, or in anticipation of effectuating, a vehicle repair covered by a vehicle warranty or a recall conducted pursuant to 49 U.S.C. s. 30118-30120, provided that the new motor vehicle dealer, distributor, or vehicle manufacturer with which that vehicle information or ownership information is shared does not sell, share, or use that information for any other purpose. As used in this paragraph, the term “vehicle information” means the vehicle identification number, make, model, year, and odometer reading, and the term “ownership information” means the name or names of the registered owner or owners and the contact information for
Section 7. Section 501.177, Florida Statutes, is created to read:

501.177 Enforcement; preemption.—

(1) ENFORCEMENT.—

(a) This subsection and subsection (2) apply only to controllers and processors that sell the personal information of consumers to third parties and that are subject to the requirements of this act.

(b) This act does not establish a private cause of action.

(c) The following are unfair and deceptive trade practices actionable under part II of this chapter solely by the Department of Legal Affairs against a controller or processor:

1. Failure to delete or correct a consumer’s personal information pursuant to this act after receiving from a controller a verifiable consumer request or directions to delete or correct, unless the controller or processor qualifies for an exception to the requirements to delete or correct under this act; and

2. Continuing to sell a consumer’s personal information after the consumer chooses to opt out or selling the personal information of a consumer age 16 or younger without obtaining the consent required by this act.

(d) If the department has reason to believe that a controller or processor has committed an act described in paragraph (c), the department, as the enforcement authority, may bring an action against such controller or processor. For the purpose of bringing an action pursuant to this act, ss. 501.211 and 501.212 do not apply. Civil penalties may be tripled if the
violation involves a consumer who the controller or processor has actual knowledge is 16 years of age or younger.

(e) After the department has notified a controller or processor in writing of an alleged violation, the department, at its discretion, may grant to the controller or processor a 45-day period to cure the alleged violation. The department may consider the number of violations, the substantial likelihood of injury to the public, or the safety of persons or property when determining whether to grant the 45-day cure period. If the controller or processor provides proof to the department that the violation has been cured to the satisfaction of the department, the department may issue a letter of guidance that indicates that the controller or processor will not be offered a 45-day cure period for any future violations. If the controller or processor fails to cure the violation within 45 days, the department may bring an action against the controller or processor for the alleged violation.

(f) A court may grant the following relief in an action brought pursuant to this act by the department:

1. Actual damages to a consumer.
2. Injunctive or declaratory relief.

(g) Liability for a tort, contract claim, or consumer protection claim which is unrelated to an action by the department does not arise solely from the failure of a controller or processor to comply with this act and evidence of such noncompliance may only be used as the basis to prove a cause of action under this section.

(h) By each February 1, the department, in conjunction and consultation with the director of the Consumer Data Privacy
Unit, shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing any actions taken by the department to enforce this act. The report must include statistics and relevant information detailing all of the following:

1. The number of complaints received.
2. The number of complaints investigated.
3. The number and type of enforcement actions taken and the outcomes of such actions.
4. The number of complaints resolved without the need for litigation.
5. The status of the development and implementation of rules to implement this act.

(i) The department may adopt rules to implement this act.

(2) JURISDICTION.—For purposes of bringing an action in accordance with this section, any person that meets the definition of a controller that collects or sells the personal information of Florida consumers, is considered to be both engaged in substantial and not isolated activities within this state and operating, conducting, engaging in, or carrying on a business, and doing business in this state, and therefore is subject to the jurisdiction of the courts of this state.

(3) PREEMPTION.—This section is a matter of statewide concern and supersedes and preempts to the state all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and county, municipality, or local agency regarding the collection, processing, or sale of consumers’ personal information by a controller or processor.

Section 8. Subsection (1) of section 16.53, Florida
Statutes, is amended, and subsection (8) is added to that section, to read:

16.53 Legal Affairs Revolving Trust Fund.—

(1) There is created in the State Treasury the Legal Affairs Revolving Trust Fund, from which the Legislature may appropriate funds for the purpose of funding investigation, prosecution, and enforcement by the Attorney General of the provisions of the Racketeer Influenced and Corrupt Organization Act, the Florida Deceptive and Unfair Trade Practices Act, the Florida False Claims Act, or state or federal antitrust laws, or the Florida Privacy Protection Act.

(8) All moneys recovered by the Attorney General for attorney fees and costs in an action for violation of the Florida Privacy Protection Act must be deposited in the fund.

Section 9. Section 16.581, Florida Statutes, is created to read:

16.581 Consumer Data Privacy Unit.—

(1) There is created in the Department of Legal Affairs the Consumer Data Privacy Unit, which shall be headed by a director who is fully accountable to the Attorney General, who shall assign the director such powers, duties, responsibilities, and functions as are necessary to ensure the greatest possible coordination, efficiency, and effectiveness of the unit in protecting the personal information of residents of this state.

(2) The unit shall serve as legal counsel in any suit or other legal action initiated in connection with the Florida Privacy Protection Act.

(3) The unit may investigate and initiate actions authorized by the Florida Privacy Protection Act.
(4) If, by its own inquiry or as a result of complaints, the unit has reason to believe that there has been a violation of the Florida Privacy Protection Act, the unit may administer oaths and affirmations, subpoena witnesses or matter, and collect evidence.

(5) The unit may refer any criminal violations so uncovered to the appropriate prosecuting authority.

(6) The unit may recover reasonable attorney fees and costs and penalties in accordance with part II of chapter 501 in any action for violation of consumer data privacy provisions in the Florida Privacy Protection Act. Such attorney fees and costs collected must be deposited in the Legal Affairs Revolving Trust Fund.

(7) All moneys recovered by the Attorney General for penalties in an action for violation of the Florida Privacy Protection Act must be deposited in the General Revenue Fund.

Section 10. This act shall take effect December 31, 2022.