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
individual consumer records that have been de-identified.

(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 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
5-01351-22

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.
(23) “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.

(24) “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.

(25) “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
material changes to the notice.
(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:
(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
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.