A bill to be entitled

An act relating to consumer data privacy; amending s. 501.171, F.S.; revising the definition of "personal information" to include additional specified information to data breach reporting requirements; creating s. 501.173, F.S.; providing definitions; providing exceptions; 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; providing that controllers must have a specified timeframe to cure any violations; providing jurisdiction; providing an effective date.

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

Section 1. 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.

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.

c. An individual's biometric information as defined in s. 501.173(1).

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

501.173 Consumer data privacy.—

(1) 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 observing the consumer's behavior.

(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 targeted advertising in conjunction with third parties or that is not covered by an exception under this section.

(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. Publicly commits to maintain and use 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;

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

4. Implements business processes to prevent inadvertent release of deidentified 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) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company,

corporation, limited liability company, association, committee, legal entity, and any other organization or group of persons acting in concert.

(l) "Personal information" means information that identifies, relates to, or describes a consumer or household, or is reasonably capable of being directly or indirectly associated or linked with, a consumer or household.

1. The term includes, but is not limited to, the following:

a. Identifiers such as a real name, alias, postal address, unique identifier, online identifier, internet protocol address, email address, account name, social security number, driver license number, passport number, or other similar identifiers.

b. Information that identifies, relates to, or describes, or could be associated with, a particular individual, including, but not limited to, a name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.

c. Characteristics of protected classifications under state or federal law.

d. Commercial information, including records of personal

property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

e. Biometric information.

f. Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet website, application, or advertisement.

g. Geolocation data.

h. Audio, electronic, visual, thermal, olfactory, or similar information.

i. Inferences drawn from any of the information identified in this paragraph to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

2. The term does not include consumer information that is:

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

b. Deidentified or aggregate consumer information.

c. Publicly and lawfully available information reasonably believed to be made available to the public in a lawful manner and without legal restrictions:

(I) From federal, state, or local government records.

(II) By a widely distributed media source.

(III) 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.

This sub-subparagraph does not include biometric information collected by a controller about a consumer without the consumer's consent.

(m) "Probabilistic identifier" means the identification of a consumer or a device to a degree of certainty of more probable than not based on any categories of personal information included in, or similar to, the categories listed under paragraph (l).

(n) "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.

(o) "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.

(p) "Pseudonymize" means the processing of personal information in a manner that renders the personal information no longer attributable to a specific consumer without the use of additional information, provided that the additional information is kept separately and is subject to technical and organizational measures to ensure that the personal information is not attributed to an identified or identifiable consumer.

(q) "Research" means scientific, systematic study and observation, including, but not limited to, basic research or applied research that is in the public interest and that adheres to all other applicable ethics and privacy laws or studies conducted in the public interest in the area of public health. Research with personal information that may have been collected from a consumer in the course of the consumer's interactions with a controller's service or device for other purposes must be:

1. Subsequently pseudonymized and deidentified, or

deidentified and in the aggregate, such that the information does not reasonably identify, relate to, or describe, or is not capable of being directly or indirectly associated or linked with, a particular consumer.

2. Made subject to technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.

3. Subject to business processes that specifically prohibit reidentification of the information.

4. Made subject to business processes to prevent inadvertent release of deidentified information.

5. Protected from any reidentification attempts.

6. Used solely for research purposes that are compatible with the context in which the personal information was collected and not used for any commercial purpose.

7. 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.

(r) "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.

(s) "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.

(t) "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.

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

(v) "Unique identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic

identifiers that can be used to identify a particular consumer, family, or device that is linked to a consumer or family. As used in this paragraph, the term "family" means a custodial parent or guardian and any minor children of whom the parent or guardian has custody, or a household.

(w) "Verifiable consumer request" means a request that is made by a consumer, by a parent or guardian on behalf of a consumer who is a minor child, or by a natural person or a person authorized by the consumer to act on the consumer's behalf, that the controller can reasonably verify pursuant to rules adopted by the department to be the consumer entitled to exercise certain rights with respect to personal information collected by the controller. 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 consumer. A verifiable consumer request is made when requested through an established account using the controller's established security features to access the account through communication features offered to consumers.

(2) EXCEPTIONS.—

(a) This section does not restrict the ability of any controller, processor, or third party to do any of the following:

1. 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.

2. Comply with federal, state, or local laws.

3. Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

4. 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.

5. Exercise legal rights or privileges.

6. Collect, use, retain, sell, share, or disclose deidentified personal information or aggregate consumer information.

(b) This section does not apply to:

1. 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. Such information cannot be sold, shared, or disclosed to another person unless otherwise authorized under this section.

2. 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.

3. Personal information collected by a controller of a natural person 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. For purposes of this subparagraph, personal information includes employee benefit information.

4. 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.

5. 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 subparagraph 4., and as long as the covered entity, business associate, or

program 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 under this section.

6. 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.

7. 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.

8. 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.

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

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

11. 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.

12. 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 subparagraph 11., 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 under this section.

13. 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.

14. 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.

15. Information collected as part of public or peer-

reviewed scientific or statistical research in the public interest.

(3) PRIVACY POLICY FOR PERSONAL INFORMATION.—

(a) A controller that collects personal information about consumers shall maintain an online privacy policy, make such policy available from its homepage, and update the information at least once every 12 months unless the privacy policy has not changed and an update is not reasonably required. The online privacy policy must include the following information:

1. Any Florida-specific consumer privacy rights.

2. A list of the categories of personal information the controller collects or has collected about consumers.

3. Of the categories identified in subparagraph 2., a list that identifies which categories of personal information the controller sells or shares or has sold or shared about consumers. If the controller does not sell or share personal information, the controller shall disclose that fact.

4. The right to request deletion or correction of certain personal information.

5. The right to opt-out of the sale or sharing to third parties.

(b) A consumer has the right to request that a controller disclose to the consumer the categories of personal information the controller collects from or about consumers. Such request does not need to be a verified consumer request.

(c) A controller that collects personal information shall, at or before the point of collection, inform consumers of the categories of personal information to be collected and the purposes for which the categories of personal information will be used. A controller that does not collect personal information directly from the consumer does not need to provide a notice at collection to the consumer if it does not sell or share the consumer's personal information.

(d) 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.

(e) 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 to implement and maintain the same or similar security procedures and practices for personal information.

(f) A controller shall adopt and implement a retention schedule that prohibits the use or retention of personal information 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 2 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 personal information about the consumer disclose the personal information that has been collected, sold, or shared by or on behalf of the controller.

(b) A consumer has the right to request that a controller that collects 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 categories of sources from which it collected the consumer's personal information.

3. The purpose for collecting, selling, or sharing the consumer's personal information.

4. The categories of third parties which the controller shares the consumer's personal information.

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

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

1. The categories of personal information about the consumer the controller sold or shared.

2. The categories of third parties to which the personal information about the consumer was sold or shared.

3. The categories of personal information about the consumer that the business disclosed to a processor.

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

(f) This subsection does not require a controller to do the following:

1. Retain any personal information about a consumer collected for a single one-time transaction if, in the ordinary course of business, that information about the consumer is not retained.

2. 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.

(g) To comply with this subsection, a controller shall, in a form that is reasonably accessible to consumers, make available two or more methods for submitting verifiable consumer requests, including, but not limited to, a toll-free number and, if the controller maintains an Internet website, a link on the homepage of the website. The controller may not require the consumer to create an account with the controller in order to make a verifiable consumer request.

(h) 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, while taking into account the complexity of the consumer's requests, provided the controller informs the consumer of any such extension within the initial 45-day response period along with the reason for the extension. The information must be delivered in a readily usable format that allows the consumer to transmit the information from

one person to another person without hindrance.

(i) A controller may provide personal information to a consumer at any time, but may not be required to provide personal information to a consumer more than twice in a 12-month period.

(j) 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.

(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.

8. Comply with a legal obligation.

9. As reasonably needed to protect the controller's interests against existing disputes, legal action, or governmental investigations.

10. Otherwise internally use the consumer's personal

information in a lawful manner that is compatible with the context in which the consumer provided the information.

(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, while taking into account the nature of the personal information and the purposes of the processing of the personal information. 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. 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) A controller that sells or shares personal information to third parties shall provide notice to consumers that this information may be sold and shared and that consumers have the

right to opt-out of the sale or sharing of their personal information.

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

(d) A controller that has received direction prohibiting the sale or sharing of the consumer's personal information or that has not received consent to sell or share a minor consumer's personal information is prohibited from selling or sharing the consumer's personal information immediately after its receipt of such direction, unless the consumer subsequently provides express authorization for the sale or sharing of the consumer's personal information.

(e) A controller does not sell or share personal information when:

1. The controller discloses personal information to another controller, a processor, or a government entity 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.

2. A consumer uses or directs the controller to intentionally disclose personal information 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, via 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.

3. The controller uses or shares an identifier for a consumer who has opted out of the sale or sharing of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale or sharing of the consumer's personal information.

4. The controller uses or shares with a processor personal information of a consumer that is necessary to perform a contracted purpose if both of the following conditions are met:

a. The controller has provided notice that the personal

information of the consumer is being used or shared in its privacy policy.

b. The processor does not further collect, sell, share, or use the personal information of the consumer except as necessary to perform the contracted purpose.

5. The controller transfers to a third party the personal information of a consumer 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 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.

(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.

2. In a form that is reasonably accessible to consumers, include a description of a consumer's rights along with a separate link to the "Do Not Sell or Share My Personal Information" Internet webpage in:

a. Its online privacy policy or policies.

b. Any Florida-specific consumer privacy rights.

3. 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 in subsection (3) and this subsection and how to direct consumers to exercise such rights.

4. For consumers who opt-out of the sale or sharing of their personal information, refrain from selling or sharing personal information collected by the controller about the consumer.

5. For consumers who opted-out of the sale or sharing 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.

6. 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) This subsection does not require a controller to include the required links and text on the homepage that the controller makes available to the public generally, if the controller maintains a separate and additional homepage that is dedicated to Florida consumers and that includes the required links and text, and the controller takes reasonable steps to ensure that Florida consumers are directed to such homepage.

(c) 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, and a controller shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to rules adopted by the department.

(8) DISCRIMINATION AGAINST CONSUMERS WHO EXERCISE PRIVACY RIGHTS.—

(a)1. A controller may not discriminate against a consumer who exercised any of the consumer's rights under this section. Discrimination under this subparagraph includes, but is not limited to:

a. Denying goods or services to the consumer.

b. Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

c. Providing a different level or quality of goods or services to the consumer.

d. Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.

2. This paragraph does not prohibit a controller from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, 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 bona fide loyalty, rewards, premium features, discounts, or club card program.

(b)1. A controller may offer financial incentives, including payments to consumers as compensation, for the collection, sale, share, or deletion of personal information.

2. A controller may offer a different price, rate, level, or quality of goods or services to the consumer if the price or difference is directly related to the value provided to the controller by the consumer's personal information or is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

3. A controller that offers any financial incentives shall notify consumers of the financial incentives.

4. A controller may enter a consumer into a financial incentive program only 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.

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

(c) A controller may offer, and a consumer may voluntarily participate in, a bona fide loyalty, rewards, premium features, discounts, or club card program.

(9) CONTRACTS AND ROLES.—

(a) Any contract between a controller and a processor must:

1. Prohibit the processor from selling or sharing the personal information;

2. Prohibit the processor from retaining, using, or disclosing the personal information other than for the purposes specified in the contract with the controller;

3. Prohibit the processor from combining the personal information that the processor receives from or on behalf of the controller with personal information that it receives from or on behalf of another person or that the processor collects from its own interaction with the consumer, provided that the processor may combine personal information to perform any purpose specified in the contract and such combination is reported to the controller;

4. 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;

5. 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

6. Upon request of the controller, require the processor to make available to the controller all information in its possession under the contract to demonstrate compliance with this section.

(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. Irrespective of the terms of the arrangement or contract, the consumer may exercise his or her rights against a controller or a processor that does not act in accordance with the terms of the contract with the controller. 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 third party or a processor must require any subcontractor to meet the same obligations of such third party or processor with respect to personal information.

(e) A third party or processor 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. A controller that discloses personal information to a third party or processor in compliance with this section is not liable or responsible if the person receiving the personal information uses it without complying with the restrictions under this section, provided that at the time of disclosing the personal information, the controller does not have actual knowledge or reason to believe that the person intends to not 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 bring a civil action against a controller, processor, or person pursuant to this section only for the following:

1. 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 violation of the duty to implement and maintain reasonable security procedures and practices.

2. 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.

3. Continuing to sell or share a consumer's personal information after the consumer chooses to opt-out pursuant to this section or 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 be brought only by or on behalf of a Florida consumer.

(e) Except as authorized under this subsection and subsection (11), liability for a tort, contract claim, or consumer protection claim which inures to the benefit of a consumer does not arise from the failure of a controller, processor or person to comply with this section and evidence of such may only be used to prove a cause of action under this subsection or subsection (11).

(11) ENFORCEMENT AND IMPLEMENTATION.—

(a) A violation of this section is an unfair and deceptive trade practice actionable under part II of chapter 501 solely by the department. If the department has reason to believe that any controller, processor, or person is in violation of this section, the department 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 and ss. 501.211 and 501.212(4) do not apply. Civil penalties may be tripled if the violation involves a consumer who the controller, processor, or person has actual knowledge is 16 years of age or younger.

(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 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 45 days to cure. If the violation is cured to the satisfaction of the department and proof is provided to the department, the department may issue a letter of guidance that indicates that the controller, processor, or person will not be offered a 45-day cure period for any future violations. 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) This subsection does not affect the private right of action provided in subsection (10).

(d) The department may adopt rules to implement this section.

(12) JURISDICTION.—For purposes of bringing an action in accordance with subsections (10) and (11), any person that meets the definition of controller as defined in this section that

collects, sells, or shares the personal information of Florida consumers, is conclusively presumed 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.

Section 3. This act shall take effect July 1, 2022.