A bill to be entitled

An act relating to consumer data privacy; creating s. 501.173, F.S.; providing applicability; providing definitions; requiring controllers that collect a consumer's personal data to disclose certain information regarding data collection and selling practices to the consumer at or before the point of collection; specifying that such information may be provided through a general privacy policy or through a notice informing the consumer that additional specific information will be provided upon a certain request; prohibiting controllers from collecting additional categories of personal information or using personal information for additional purposes without notifying the consumer; requiring controllers that collect personal information to implement reasonable security procedures and practices to protect the information; authorizing consumers to request controllers to disclose the specific personal information the controller has collected about the consumer; requiring controllers to make available two or more methods for consumers to request their personal information; requiring controllers to provide such information free of charge within a certain timeframe and in a certain format upon receiving a verifiable consumer request;

specifying requirements for third parties with respect to consumer information acquired or used; providing construction; authorizing consumers to request controllers to delete or correct personal information the controllers have collected about the consumers; providing exceptions; specifying requirements for controllers to comply with deletion or correction requests; authorizing consumers to opt out of third-party disclosure of personal information collected by a controller; prohibiting controllers from selling or disclosing the personal information of consumers younger than a certain age, except under certain circumstances; prohibiting controllers from selling or sharing a consumer's information if the consumer has opted out of such disclosure; prohibiting controllers from taking certain actions to retaliate against consumers who exercise certain rights; providing applicability; providing that a contract or agreement that waives or limits certain consumer rights is void and unenforceable; providing for civil actions and a private right of action for consumers under certain circumstances; providing civil remedies; authorizing the Department of Legal Affairs to bring an action under the Florida Unfair or Deceptive Trade Practices Act and to adopt rules; requiring the department to

submit an annual report to the Legislature; providing report requirements; providing that controllers must have a specified timeframe to cure any violations; providing jurisdiction; declaring that the act is matter of statewide concern; preempting the collection, processing, sharing, and sale of consumer personal information to the state; amending s. 501.171, F.S.; revising the definition of "personal information"; providing an effective date.

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

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

501.173 Consumer data privacy.—

(1) APPLICABILITY.—This section applies to any entity that meets the definition of controller, processor, or third party, and that buys, sells, or shares personal information of Florida consumers. This section does not apply to entities that do not buy, sell, or share personal information of Florida consumers and such entities do not have to comply with this section. This section also does not apply to:

(a) Personal information collected and transmitted that is necessary for the sole purpose of sharing such personal information with a financial service provider solely to

facilitate short term, transactional payment processing for the purchase of products or services.

(b) Personal information collected, used, retained, sold, shared, or disclosed as deidentified personal information or aggregate consumer information.

(c) Compliance with federal, state, or local laws.

(d) Compliance with a civil, criminal, or regulatory inquiry, investigation, subpoena, or summons by federal, state, or local authorities.

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

(f) Exercising or defending legal claims.

(g) Personal information collected through the controller's direct interactions with the consumer, if collected in accordance with the provisions of this section, that is used by the controller or the processor that the controller directly contracts with for advertising or marketing services to advertise or market products or services that are produced or offered directly by the controller. Such information may not be sold, shared, or disclosed unless otherwise authorized under this section.

(h) Personal information of a person acting in the role of a job applicant, employee, owner, director, officer, contractor,

volunteer, or intern of a controller, that is collected by a controller, to the extent the personal information is collected and used solely within the context of the person's role or former role with the controller.

(i) 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.

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

(k) 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.

(l) 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.

(m) 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.

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

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

(p) 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.

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

(r) 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.

(s) 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.

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

individuals necessary to carry out the research purpose and subsequently deidentified.

(u) Personal information disclosed for the purpose of responding to an alert of a present risk of harm to a person or property or prosecuting those responsible for that activity.

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

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

(x) Personal information transferred by a controller to a third party as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that information is used or shared consistently with this section. If a third party materially alters how it uses or shares the

personal information of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that consumers can easily exercise choices consistent with this section.

(y) Personal information necessary to fulfill the terms of a written warranty when such warranty was purchased by the consumer or the product that is warranted was purchased by the consumer. Such information may not be sold or shared unless otherwise authorized under this section.

(z) Personal information necessary for a product recall for a product purchased or owned by the consumer conducted in accordance with federal law. Such information may not be sold or shared unless otherwise authorized under this section.

(aa) Personal information processed solely for the purpose of independently measuring or reporting advertising or content performance, reach, or frequency pursuant to a contract with a controller that collected personal information in accordance with this section. Such information may not be sold or shared unless otherwise authorized under this section.

(2) DEFINITIONS.—As used in this section, the term:

(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which the identity of an individual consumer has been removed and is not

reasonably capable of being directly or indirectly associated or linked with, any consumer, household, or device. The term does not include personal information that has been deidentified.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics 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 or actions.

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

(e) "Controller" means:

1. A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:

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

b. Does business in this state;

c. Collects personal information about consumers, or is the entity on behalf of which such information is collected;

d. Determines the purposes and means of processing personal information about consumers alone or jointly with others; and

e. Satisfies at least two of the following thresholds:

(I) Has global annual gross revenues in excess of $50 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

(II) Annually buys, sells, or shares the personal information of 50,000 or more consumers, households, and devices for the purpose of targeted advertising in conjunction with third parties. The 50,000 total only includes personal information that is bought, sold, or shared within the previous 12 months.

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

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

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

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

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

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

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

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

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

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

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

(i) "Genetic information" means an individual's deoxyribonucleic acid (DNA).

(j) "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.

(k) "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.

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

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

2. Deidentified or aggregate consumer information.

3. Publicly and lawfully available information reasonably believed to be made available to the general public:

a. From federal, state, or local government records.

b. By a widely distributed media source.

c. By the consumer or by someone to whom the consumer disclosed the information unless the consumer has purposely and effectively restricted the information to a certain audience on a private account.

(m) "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.

(n) "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, as permitted by this section.

(o) "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.

(p) "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 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.

(q) "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.

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

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

(3) CONSUMER DATA COLLECTION REQUIREMENTS AND RESPONSIBILITIES.—

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

1. Any Florida-specific consumer privacy rights.

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

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

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

(b) A controller that collects personal information from the consumer shall, at or before the point of collection, inform, or direct the processor to inform, consumers of the categories of personal information to be collected and the

purposes for which the categories of personal information will be used.

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

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

(e) A controller shall adopt and implement a retention schedule that prohibits the use or retention of personal information not subject to an exemption by the controller or processor after the satisfaction of the initial purpose for which such information was collected or obtained, after the expiration or termination of the contract pursuant to which the information was collected or obtained, or 3 years after the consumer's last interaction with the controller. This paragraph does not apply to personal information reasonably used or retained to do any of the following:

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

2. Provide a good or service requested by the consumer, or

reasonably anticipate the request of such good or service within the context of a controller's ongoing business relationship with the consumer.

3. Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activity or access.

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

5. 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.

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

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

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

9. Assure the physical security of persons or property.

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

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

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

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

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

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

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

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

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

(d) The controller shall deliver the information required or act on the request in this subsection to a consumer free of

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

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

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

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

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

1. A controller that receives a verifiable consumer request to delete the consumer's personal information shall delete the consumer's personal information from its records and direct any processors to delete such information within 90

calendar days of receipt of the verifiable consumer request.

2. 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:

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

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

c. Provide a good or service requested by the consumer, or reasonably anticipate the request of such good or service within the context of a controller's ongoing business relationship with the consumer, or otherwise perform a contract between the controller and the consumer.

d. Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activity or access.

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

f. 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.

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

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

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

j. Assure the physical security of persons or property.

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

information through such mechanism. 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 correct 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. Detect security threats or incidents; protect against malicious, deceptive, fraudulent, unauthorized, or illegal activity or access; or prosecute those responsible for such activity or access.

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

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

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

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

8. Assure the physical security of persons or property.

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

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

(b) Notwithstanding paragraph (a), a controller may not sell or share the personal information of a minor consumer if the controller has actual knowledge that the consumer is not 18 years of age or older. However, if a consumer who is between 13 and 18 years of age, or if the parent or guardian of a consumer who is 12 years of age or younger, has affirmatively authorized the sale or sharing of such consumer's personal information, then a controller may sell or share such information in accordance with this section. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age. A controller that complies with the verifiable parental consent requirements of the Children's Online Privacy Protection Act, 15 U.S.C. s. 6501 et seq., shall be deemed compliant with any obligation to obtain parental consent.

(c) A controller that has received direction from a consumer opting-out of the sale or sharing of the consumer's personal information is prohibited from selling or sharing the

consumer's personal information beginning 4 calendar days after receipt of such direction, unless the consumer subsequently provides express authorization for the sale or sharing of the consumer's personal information.

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

(a) A controller shall:

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

2. For consumers who opted-out of the sale or sharing of their personal information, respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale or sharing of the consumer's personal information.

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

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

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

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

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

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

(9) CONTRACTS AND ROLES.—

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

1. Prohibit the processor from selling, sharing, retaining, using, or disclosing the personal information for any purpose that violates this section;

2. Govern the processor's personal information processing procedures with respect to processing performed on behalf of the controller, including processing instructions, the nature and purpose of processing, the type of information subject to processing, the duration of processing, and the rights and obligations of both the controller and processor;

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

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

(b) Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal information is to be processed. The contract between a

controller and processor must reflect their respective roles and relationships related to handling personal information. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal information remains a processor.

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

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

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

(f) Any provision of a contract or agreement of any kind that waives or limits in any way a consumer's rights under this section, including, but not limited to, any right to a remedy or means of enforcement, is deemed contrary to public policy and is void and unenforceable. This section does not prevent a consumer from declining to exercise the consumer's rights under this section.

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

(a) A Florida consumer may only bring a civil action pursuant to this section against:

1. A controller, processor, or third party who has global annual gross revenues of at least $50 million, but not more than $500 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index. Upon prevailing, the Florida consumer may be awarded relief described in paragraph (c), but may not be awarded attorney fees or costs. Any private claim solely based on this section against a controller, processor, or third party who has global annual gross revenues of less than $50 million, is barred.

2. A controller, processor, or third party who has global annual gross revenues of more than $500 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index. Upon prevailing, the Florida consumer may be awarded relief described in paragraph (c), and shall recover reasonable attorney fees and costs.

(b) A Florida consumer may only bring a civil action pursuant to this section against a controller, processor, or third party who meets a threshold in paragraph (a) for the following actions:

1. Failure to delete or correct the 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 third

party qualifies for an exception to the requirements to delete or correct under this section.

2. Continuing to sell or share the consumer's personal information after the consumer chooses to opt-out pursuant to this section.

3. Selling or sharing the personal information of the consumer age 18 or younger without obtaining consent as required by this section.

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

1. Statutory 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.

(d) Upon prevailing, a controller, processor, or third party may only be awarded attorney fees if the court finds that there was a complete absence of a justiciable issue of either law or fact raised by the consumer or if the court finds bad faith on the part of the consumer, including if the consumer is not a Florida consumer.

(e) A consumer must commence a civil action for a claim under this section within 1 year after discovery of the violation.

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

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

(h) In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the length of time over which the misconduct occurred, and the defendant's assets, liability, and net worth.

(11) ENFORCEMENT AND IMPLEMENTATION BY THE DEPARTMENT.—

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

1. Involves a Florida consumer who the controller, processor, or third party has actual knowledge is 18 years of age or younger; or

2. Is based on paragraph (10)(b).

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

(c) Any action brought by the department may only be brought on behalf of a Florida consumer.

(d) By February 1 of each year, the department shall submit a report to the President of the Senate and the Speaker of the House of Representatives describing any actions taken by

the department to enforce this section. The report shall include statistics and relevant information detailing:

1. The number of complaints received;

2. The number and type of enforcement actions taken and the outcomes of such actions;

3. The number of complaints resolved without the need for litigation; and

4. The status of the development and implementation of rules to implement this section.

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

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

(13) PREEMPTION.—This section is a matter of statewide concern and supersedes all rules, regulations, codes, ordinances, and other laws adopted by a city, county, city and

county, municipality, or local agency regarding the collection, processing, sharing, or sale of consumer personal information by a controller or processor. The regulation of the collection, processing, sharing, or sale of consumer personal information by a controller or processor is preempted to the state.

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

501.171 Security of confidential personal information.—

(1) DEFINITIONS.—As used in this section, the term:

(g)1. "Personal information" means either of the following:

a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual:

(I) A social security number;

(II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity;

(III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account;

(IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or

diagnosis by a health care professional; or

(V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual.

(VI) An individual's biometric information or genetic information as defined in s. 501.173(2).

b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account.

2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.

Section 3. This act shall take effect January 1, 2023.