CHAPTER 2023-201

Committee Substitute for
Committee Substitute for Senate Bill No. 262

An act relating to technology transparency; creating s. 112.23, F.S.; defining terms; prohibiting officers or salaried employees of governmental entities from using their positions or state resources to make certain requests of social media platforms; prohibiting governmental entities from initiating or maintaining agreements or working relationships with social media platforms under a specified circumstance; providing exceptions; creating s. 501.1735, F.S.; providing definitions; prohibiting certain conduct by an online platform that provides online services, products, games, or features likely to be predominantly accessed by children; providing exceptions; providing for enforcement; providing construction; authorizing the department to bring an action under the Florida Deceptive and Unfair Trade Practices Act; providing for civil penalties; providing that the department may grant an online platform a timeframe to cure any violations; providing jurisdiction; providing directives to the Division of Law Revision; creating s. 501.701, F.S.; providing a short title; creating s. 501.702, F.S.; defining terms; creating s. 501.703, F.S.; providing applicability; creating s. 501.704, F.S.; providing exemptions; creating s. 501.705, F.S.; providing that a consumer may submit requests to controllers to exercise specified rights; requiring controllers to comply with certain authenticated consumer requests; prohibiting certain devices from being used for surveillance purposes without the express authorization of the consumer under certain circumstances; creating s. 501.706, F.S.; providing timeframes within which controllers must respond to consumer requests; providing notice requirements for controllers that cannot take action regarding a consumer's request; providing that controllers are not required to comply with certain consumer requests; providing notice requirements for controllers' compliance with consumer requests; requiring responses to consumer requests to be made free of charge; providing exceptions; specifying the methods by which controllers may be considered to be in compliance with consumer requests for the controller to delete their personal data; creating s. 501.707, F.S.; requiring controllers to establish a process for consumers to appeal the controller's refusal to take action on the consumer's request within a specified timeframe; providing requirements for such process; creating s. 501.708, F.S.; providing that contracts or agreements that waive or limit specified consumer rights are void and unenforceable; creating s. 501.709, F.S.; requiring controllers to establish methods for submitting consumer requests; prohibiting controllers from requiring consumers to create new accounts to exercise their consumer rights; requiring controllers to provide a certain mechanism on their websites for consumers to submit certain requests; creating s. 501.71, F.S.; requiring controllers to limit the collection of personal data according to certain parameters; requiring controllers to establish, implement, and maintain specified

practices regarding personal data; prohibiting controllers from taking certain actions regarding a consumer's personal data; prohibiting controllers from discriminating against consumers exercising their consumer rights; providing construction; requiring a controller that operates a search engine to make certain information available on its webpage; creating s. 501.711, F.S.; requiring controllers to provide consumers with privacy notices that meet certain requirements; requiring controllers that engage in the sale of sensitive or biometric personal data to provide notices that meet certain requirements; requiring controllers that sell personal data or process personal data for targeted advertising to disclose certain information; prohibiting controllers from collecting additional categories of personal information or using such information for additional purposes without providing specified notice; creating s. 501.712, F.S.; requiring processors to adhere to controller instructions and to assist the controller in meeting or complying with certain requirements; providing requirements for contracts between controllers and processors regarding data processing procedures; providing construction; providing that the determination of whether a person is acting as a controller or processor is a fact-based determination; creating s. 501.713, F.S.; requiring controllers to conduct and document data protection assessments of specified processing activities involving personal data; providing requirements for such assessments; providing applicability; creating s. 501.714, F.S.; requiring controllers in possession of deidentified data to take certain actions; providing construction; providing that specified consumer rights and controller duties do not apply to pseudonymous data or aggregate consumer information under certain circumstances; requiring controllers that disclose pseudonymous data, deidentified data, or aggregate consumer information to exercise reasonable oversight and take appropriate steps to address breaches of contractual agreements; creating s. 501.715, F.S.; requiring certain persons to receive consumer consent before engaging in the sale of sensitive personal data; requiring a specified notice; providing for penalties; creating s. 501.716, F.S.; providing exemptions for specified controller or processor uses of consumer personal data; providing that controllers or processors may provide personal data concerning a consumer to certain covered persons; creating s. 501.717, F.S.; authorizing controllers and processors to collect, use, or retain data for specified purposes; providing that certain requirements do not apply if such compliance would violate certain laws; creating s. 501.718, F.S.; providing circumstances under which processors are not in violation of this act for the disclosure of personal data to a third-party controller or processor; providing that third-party controllers or processors that comply with this part are not liable for violations committed by controllers or processors from whom they receive personal data; creating s. 501.719, F.S.; providing requirements for the processing of certain personal data by controllers; requiring controllers and processors to adopt and implement a retention schedule that meets certain requirements; requiring controllers or processors that process certain personal data to demonstrate that such processing qualifies for a specified exemption; creating s. 501.72, F.S.; authorizing the Department of Legal Affairs to bring an action under the

Florida Deceptive and Unfair Trade Practices Act for violations of the act; providing for civil penalties; providing for enhanced civil penalties for certain violations; authorizing the department to grant a specified timeframe within which an alleged violation may be cured; providing an exception; providing certain factors the department may take into consideration; requiring the department to make a report regarding certain enforcement actions publicly available on the department's website; providing requirements for the report; requiring the department to adopt rules; authorizing the department to collaborate and cooperate with specified enforcement authorities; specifying that the act does not create a private cause of action; authorizing the department to employ or use outside legal counsel for specified purposes; providing for jurisdiction; creating s. 501.721, F.S.; declaring that the act is a matter of statewide concern; preempting the collection, processing, sharing, and sale of consumer personal data to the state; amending s. 501.171, F.S.; revising the definition of the term "personal information"; amending s. 16.53, F.S.; revising the purpose of the Legal Affairs Revolving Trust Fund; requiring that certain attorney fees, costs, and penalties recovered by the Attorney General be deposited in the trust fund; providing effective dates.

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

Section 1. Effective July 1, 2023, section 112.23, Florida Statutes, is created to read:

112.23 Government-directed content moderation of social media platforms prohibited.—

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

(a) "Governmental entity" means any officer or employee of a state, county, district, authority, municipality, department, agency, division, board, bureau, commission, or other separate unit of government created or established by law, and includes any other public or private entity acting on behalf of such governmental entity.

(b) "Social media platform" means a form of electronic communication through which users create online communities or groups to share information, ideas, personal messages, and other content.

(2) A governmental entity may not communicate with a social media platform to request that it remove content or accounts from the social media platform.

(3) A governmental entity may not initiate or maintain any agreements or working relationships with a social media platform for the purpose of content moderation.

(4) Subsections (2) and (3) do not apply if the governmental entity or an officer or an employee acting on behalf of a governmental entity is acting as part of any of the following:

(a) Routine account management of the governmental entity's account, including, but not limited to, the removal or revision of the governmental entity's content or account or identification of accounts falsely posing as a governmental entity, officer, or salaried employee.

(b) An attempt to remove content that pertains to the commission of a crime or violation of this state's public records law.

(c) An attempt to remove an account that pertains to the commission of a crime or violation of this state's public records law.

(d) An investigation or inquiry related to an effort to prevent imminent bodily harm, loss of life, or property damage.

Section 2. Section 501.1735, Florida Statutes, is created to read:

501.1735 Protection of children in online spaces.—

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

(a) "Child" or "children" means a consumer or consumers who are under 18 years of age.

(b) "Collect" means to buy, rent, gather, obtain, receive, save, store, or access any personal information pertaining to a child.

(c) "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice and includes, but is not limited to, any practice the Federal Trade Commission refers to as a dark pattern.

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

(e) "Online platform" means a social media platform as defined in s. 112.23(1), online game, or online gaming platform.

(f) "Personal information" means information that is linked or reasonably linkable to an identified or identifiable child, including biometric information and unique identifiers to the child.

(g) "Precise geolocation data" means information identified through technology which enables the online platform to collect specific location data which directly identifies the specific location of a child with precision and accuracy within a radius of 1,750 feet.

(h) "Processing" means any operation or set of operations performed on personal information or on sets of personal information, regardless of whether by automated means.

(i) "Profile" or "profiling" means any form of automated processing performed on personal information to evaluate, analyze, or predict personal aspects relating to the economic situation, health, personal preferences, interests, reliability, behavior, location, or movements of a child.

(j) "Sell" means to sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, a child's personal information or information that relates to a group or category of children by an online platform to another online platform or an affiliate or third party for monetary or other valuable consideration.

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

1. Allowing a third party to advertise or market based on a child'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 an online platform and a third party for advertising or marketing.

(l) "Substantial harm or privacy risk to children" means the processing of personal information in a manner that may result in any reasonably foreseeable substantial physical injury, economic injury, or offensive intrusion into the privacy expectations of a reasonable child under the circumstances, including:

1. Mental health disorders or associated behaviors, including the promotion or exacerbation of self-harm, suicide, eating disorders, and substance abuse disorders;

2. Patterns of use that indicate or encourage addictive behaviors;

3. Physical violence, online bullying, and harassment;

4. Sexual exploitation, including enticement, sex trafficking, and sexual abuse and trafficking of online sexual abuse material;

5. Promotion and marketing of tobacco products, gambling, alcohol, or narcotic drugs as defined in s. 102 of the Controlled Substances Act, 21 U.S.C. 802; or

6. Predatory, unfair, or deceptive marketing practices or other financial harms.

(2) PROHIBITIONS.—An online platform that provides an online service, product, game, or feature likely to be predominantly accessed by children may not:

(a) Process the personal information of any child if the online platform has actual knowledge of or willfully disregards that the processing may result in substantial harm or privacy risk to children.

(b) Profile a child unless both of the following criteria are met:

1. The online platform can demonstrate it has appropriate safeguards in place to protect children.

2.a. Profiling is necessary to provide the online service, product, or feature requested for the aspects of the online service, product, or feature with which the child is actively and knowingly engaged; or

b. The online platform can demonstrate a compelling reason that profiling does not pose a substantial harm or privacy risk to children.

(c) Collect, sell, share, or retain any personal information that is not necessary to provide an online service, product, or feature with which a child is actively and knowingly engaged unless the online platform can demonstrate a compelling reason that collecting, selling, sharing, or retaining the personal information does not pose a substantial harm or privacy risk to children.

(d) Use personal information of a child for any reason other than the reason for which the personal information was collected, unless the online platform can demonstrate a compelling reason that the use of the personal information does not pose a substantial harm or privacy risk to children.

(e) Collect, sell, or share any precise geolocation data of children unless the collection of the precise geolocation data is strictly necessary for the online platform to provide the service, product, or feature requested and then only for the limited time that the collection of the precise geolocation data is necessary to provide the service, product, or feature.

(f) Collect any precise geolocation data of a child without providing an obvious sign to the child for the duration of the collection that the precise geolocation data is being collected.

(g) Use dark patterns to lead or encourage children to provide personal information beyond what personal information would otherwise be reasonably expected to be provided for that online service, product, game, or feature; to forego privacy protections; or to take any action that the online platform has actual knowledge of or willfully disregards that may result in substantial harm or privacy risk to children.

(h) Use any personal information collected to estimate age or age range for any other purpose or retain that personal information longer than necessary to estimate age. The age estimate must be proportionate to the risks and data practice of an online service, product, or feature.

(3) BURDEN OF PROOF.—If an online platform processes personal information pursuant to subsection (2), the online platform bears the burden of demonstrating that such processing does not violate subsection (2).

(4) ENFORCEMENT AND IMPLEMENTATION BY THE DEPARTMENT.—

(a) Any violation of subsection (2) is an unfair and deceptive trade practice actionable under part II of chapter 501 solely by the department against an online platform. If the department has reason to believe that an online platform is in violation of subsection (2), the department, as the enforcing authority, may bring an action against such online platform 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. In addition to other remedies under part II of chapter 501, the department may collect a civil penalty of up to $50,000 per violation of this section. Civil penalties may be tripled for any violation involving a Florida child who the online platform has actual knowledge is under 18 years of age.

(b) After the department has notified an online platform in writing of an alleged violation, the department may in its discretion grant a 45-day period to cure the alleged violation. If the violation is cured to the satisfaction of the department and proof of such cure is provided to the department, the department may not bring an action for the alleged violation but in its discretion may issue a letter of guidance that indicates that the online platform will not be offered a 45-day cure period for any future violations. If the online platform fails to cure the violation within 45 calendar days, the department may bring an action against the online platform for the alleged violation.

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

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

(e) Liability for a tort, contract claim, or consumer protection claim that is unrelated to an action brought under this subsection does not arise solely from the failure of an online platform to comply with this section.

(f) This section does not establish a private cause of action.

(5) JURISDICTION.—For purposes of bringing an action pursuant to this section, any person who meets the definition of online platform which operates an online service, product, game, or feature likely to be predominantly accessed by children and accessible by Florida children located in this state 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.

Section 3. The Division of Law Revision is directed to:

(1) Redesignate current parts V, VI, and VII of chapter 501, Florida Statutes, as parts VI, VII, and VIII of chapter 501, Florida Statutes, respectively; and

(2) Create a new part V of chapter 501, Florida Statutes, consisting of ss. 501.701-501.721, Florida Statutes, entitled "Data Privacy and Security."

Section 4. Section 501.701, Florida Statutes, is created to read:

501.701 Short title.—This part may be cited as the "Florida Digital Bill of Rights."

Section 5. Section 501.702, Florida Statutes, is created to read:

501.702 Definitions.—As used in this part, the term:

(1) "Affiliate" means a legal entity that controls, is controlled by, or is under common control with another legal entity or that shares common branding with another legal entity. For purposes of this subsection, the term "control" or "controlled" means any of the following:

(a) The ownership of, or power to vote, more than 50 percent of the outstanding shares of any class of voting security of a company.

(b) The control in any manner over the election of a majority of the directors or of individuals exercising similar functions.

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

(2) "Aggregate consumer information" means information that relates to a group or category of consumers, from which 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 information about a group or category of consumers used to facilitate targeted advertising or the display of ads online. The term does not include personal information that has been deidentified.

(3) "Authenticate" or "authenticated" means to verify or the state of having been verified, respectively, through reasonable means that the consumer who is entitled to exercise the consumer's rights under s. 501.705 is the same consumer exercising those consumer rights with respect to the personal data at issue.

(4) "Biometric data" means data generated by automatic measurements of an individual's biological characteristics. The term includes fingerprints, voiceprints, eye retinas or irises, or other unique biological patterns or characteristics used to identify a specific individual. The term does not include physical or digital photographs, video or audio recordings or data generated from video or audio recordings, or information collected, used, or

stored for health care treatment, payment, or operations under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(5) "Business associate" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(6) "Child" means an individual younger than 18 years of age.

(7) "Consent," when referring to a consumer, means a clear affirmative act signifying a consumer's freely given, specific, informed, and unambiguous agreement to process personal data relating to the consumer. The term includes a written statement, including a statement written by electronic means, or any other unambiguous affirmative act. The term does not include any of the following:

(a) Acceptance of a general or broad terms of use or similar document that contains descriptions of personal data processing along with other, unrelated information.

(b) Hovering over, muting, pausing, or closing a given piece of content.

(c) Agreement obtained through the use of dark patterns.

(8) "Consumer" means an individual who is a resident of or is domiciled in this state acting only in an individual or household context. The term does not include an individual acting in a commercial or employment context.

(9) "Controller" means:

(a) A sole proprietorship, partnership, limited liability company, corporation, association, or legal entity that meets the following requirements:

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

2. Conducts business in this state;

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

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

5. Makes in excess of $1 billion in global gross annual revenues; and

6. Satisfies at least one of the following:

a. Derives 50 percent or more of its global gross annual revenues from the sale of advertisements online, including providing targeted advertising or the sale of ads online;

b. Operates a consumer smart speaker and voice command component service with an integrated virtual assistant connected to a cloud computing service that uses hands-free verbal activation. For purposes of this sub-subparagraph, a consumer smart speaker and voice command component service does not include a motor vehicle or speaker or device associated with or connected to a vehicle which is operated by a motor vehicle manufacturer or a subsidiary or affiliate thereof; or

c. Operates an app store or a digital distribution platform that offers at least 250,000 different software applications for consumers to download and install.

(b) Any entity that controls or is controlled by a controller. As used in this paragraph, the term "control" means:

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

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

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

(10) "Covered entity" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(11) "Dark pattern" means a user interface designed or manipulated with the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice. The term includes any practice the Federal Trade Commission refers to as a dark pattern.

(12) "Decision that produces a legal or similarly significant effect concerning a consumer" means a decision made by a controller which results in the provision or denial by the controller of any of the following:

(a) Financial and lending services.

(b) Housing, insurance, or health care services.

(c) Education enrollment.

(d) Employment opportunities.

(e) Criminal justice.

(f) Access to basic necessities, such as food and water.

(13) "Deidentified data" means data that cannot reasonably be linked to an identified or identifiable individual or a device linked to that individual.

(14) "Health care provider" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(15) "Health record" means any written, printed, or electronically recorded material maintained by a health care provider in the course of providing health care services to an individual which concerns the individual and the services provided. The term includes any of the following:

(a) The substance of any communication made by an individual to a health care provider in confidence during or in connection with the provision of health care services.

(b) Information otherwise acquired by the health care provider about an individual in confidence and in connection with health care services provided to the individual.

(16) "Identified or identifiable individual" means a consumer who can be readily identified, directly or indirectly.

(17) "Known child" means a child under circumstances of which a controller has actual knowledge of, or willfully disregards, the child's age.

(18) "Nonprofit organization" means any of the following:

(a) An organization exempt from federal taxation under s. 501(a) of the Internal Revenue Code of 1986 by virtue of being listed as an exempt organization under s. 501(c)(3), s. 501(c)(4), s. 501(c)(6), or s. 501(c)(12) of that code.

(b) A political organization.

(19) "Personal data" means any information, including sensitive data, which is linked or reasonably linkable to an identified or identifiable individual. The term includes pseudonymous data when the data is used by a controller or processor in conjunction with additional information that reasonably links the data to an identified or identifiable individual. The term does not include deidentified data or publicly available information.

(20) "Political organization" means a party, a committee, an association, a fund, or any other organization, regardless of whether incorporated, organized and operated primarily for the purpose of influencing or attempting to influence any of the following:

(a) The selection, nomination, election, or appointment of an individual to a federal, state, or local public office or an office in a political organization, regardless of whether the individual is selected, nominated, elected, or appointed.

(b) The election of a presidential or vice-presidential elector, regardless of whether the elector is selected, nominated, elected, or appointed.

(21) "Postsecondary education institution" means a Florida College System institution, state university, or nonpublic postsecondary education institution that receives state funds.

(22) "Precise geolocation data" means information derived from technology, including global positioning system level latitude and longitude coordinates or other mechanisms, which directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. The term does not include the content of communications or any data generated by or connected to an advanced utility metering infrastructure system or to equipment for use by a utility.

(23) "Process" or "processing" means an operation or set of operations performed, whether by manual or automated means, on personal data or on sets of personal data, such as the collection, use, storage, disclosure, analysis, deletion, or modification of personal data.

(24) "Processor" means a person who processes personal data on behalf of a controller.

(25) "Profiling" means any form of solely automated processing performed on personal data to evaluate, analyze, or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.

(26) "Protected health information" has the same meaning as in 45 C.F.R. s. 160.103 and the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(27) "Pseudonymous data" means any information that cannot be attributed to a specific individual without the use of additional information, provided that the additional information is kept separately and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

(28) "Publicly available information" means information lawfully made available through government records, or information that a business has a reasonable basis for believing is lawfully made available to the general public through widely distributed media, by a consumer, or by a person to whom a consumer has disclosed the information, unless the consumer has restricted the information to a specific audience.

(29) "Sale of personal data" means the sharing, disclosing, or transferring of personal data for monetary or other valuable consideration by the controller to a third party. The term does not include any of the following:

(a) The disclosure of personal data to a processor who processes the personal data on the controller's behalf.

(b) The disclosure of personal data to a third party for purposes of providing a product or service requested by the consumer.

(c) The disclosure of information that the consumer:

1. Intentionally made available to the general public through a mass media channel; and

2. Did not restrict to a specific audience.

(d) The disclosure or transfer of personal data to a third party as an asset that is part of a merger or an acquisition.

(30) "Search engine" means technology and systems that use algorithms to sift through and index vast third-party websites and content on the Internet in response to search queries entered by a user. The term does not include the license of search functionality for the purpose of enabling the licensee to operate a third-party search engine service in circumstances where the licensee does not have legal or operational control of the search algorithm, the index from which results are generated, or the ranking order in which the results are provided.

(31) "Sensitive data" means a category of personal data which includes any of the following:

(a) Personal data revealing an individual's racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status.

(b) Genetic or biometric data processed for the purpose of uniquely identifying an individual.

(c) Personal data collected from a known child.

(d) Precise geolocation data.

(32) "State agency" means any department, commission, board, office, council, authority, or other agency in the executive branch of state government created by the State Constitution or state law. The term includes a postsecondary education institution.

(33) "Targeted advertising" means displaying to a consumer an advertisement selected based on personal data obtained from that consumer's activities over time across affiliated or unaffiliated websites and online applications used to predict the consumer's preferences or interests. The term does not include an advertisement that is:

(a) Based on the context of a consumer's current search query on the controller's own website or online application; or

(b) Directed to a consumer search query on the controller's own website or online application in response to the consumer's request for information or feedback.

(34) "Third party" means a person, other than the consumer, the controller, the processor, or an affiliate of the controller or processor.

(35) "Trade secret" has the same meaning as in s. 812.081.

(36) "Voice recognition feature" means the function of a device which enables the collection, recording, storage, analysis, transmission, interpretation, or other use of spoken words or other sounds.

Section 6. Section 501.703, Florida Statutes, is created to read:

501.703 Applicability.—

(1) This part applies only to a person who:

(a) Conducts business in this state or produces a product or service used by residents of this state; and

(b) Processes or engages in the sale of personal data.

(2) This part does not apply to any of the following:

(a) A state agency or a political subdivision of the state.

(b) A financial institution or data subject to Title V, Gramm-Leach-Bliley Act, 15 U.S.C. ss. 6801 et seq.

(c) A covered entity or business associate governed by the privacy, security, and breach notification regulations issued by the United States Department of Health and Human Services, 45 C.F.R. parts 160 and 164, established under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq., and the Health Information Technology for Economic and Clinical Health Act, Division A, Title XIII and Division B, Title IV, Pub. L. No. 111-5.

(d) A nonprofit organization.

(e) A postsecondary education institution.

(f) The processing of personal data:

1. By a person in the course of a purely personal or household activity.

2. Solely for measuring or reporting advertising performance, reach, or frequency.

(3) A controller or processor that complies with the authenticated parental consent requirements of the Children's Online Privacy Protection

Act, 15 U.S.C. ss. 6501 et seq., with respect to data collected online, is considered to be in compliance with any requirement to obtain parental consent under this part.

Section 7. Section 501.704, Florida Statutes, is created to read:

501.704 Exemptions.—All of the following information is exempt from this part:

(1) Protected health information under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(2) Health records.

(3) Patient identifying information for purposes of 42 U.S.C. s. 290dd-2.

(4) Identifiable private information:

(a) For purposes of the federal policy for the protection of human subjects under 45 C.F.R. part 46;

(b) Collected as part of human subjects research under the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or the protection of human subjects under 21 C.F.R. parts 50 and 56; or

(c) That is personal data used or shared in research conducted in accordance with this part or other research conducted in accordance with applicable law.

(5) Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. ss. 11101 et seq.

(6) Patient safety work product for purposes of the Patient Safety and Quality Improvement Act of 2005, 42 U.S.C. ss. 299b-21 et seq.

(7) Information derived from any of the health-care-related information listed in this section which is deidentified in accordance with the requirements for deidentification under the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(8) Information originating from, and intermingled to be indistinguishable with, or information treated in the same manner as, information exempt under this section which is maintained by a covered entity or business associate as defined by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq. or by a program or a qualified service organization as defined by 42 U.S.C. s. 290dd-2.

(9) Information included in a limited data set as described by 45 C.F.R. s. 164.514(e), to the extent that the information is used, disclosed, and maintained in the manner specified by 45 C.F.R. s. 164.514(e).

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

(11) Information collected or used only for public health activities and purposes as authorized by the Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

(12) The collection, maintenance, disclosure, sale, communication, or use of any personal data bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living by a consumer reporting agency or furnisher that provides information for use in a consumer report, or by a user of a consumer report, but only to the extent that the activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. ss. 1681 et seq.

(13) Personal data collected, processed, sold, or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq.

(14) Personal data regulated by the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. s. 1232g.

(15) Personal data collected, processed, sold, or disclosed in compliance with the Farm Credit Act of 1971, 12 U.S.C. ss. 2001 et seq.

(16) Data processed or maintained in the course of an individual applying to, being employed by, or acting as an agent or independent contractor of a controller, processor, or third party, to the extent that the data is collected and used within the context of that role.

(17) Data processed or maintained as the emergency contact information of an individual under this part which is used for emergency contact purposes.

(18) Data that is processed or maintained and that is necessary to retain to administer benefits for another individual which relates to an individual described in subsection (16) and which is used for the purposes of administering those benefits.

(19) Personal data collected and transmitted which is necessary for the sole purpose of sharing such personal data with a financial service provider solely to facilitate short-term, transactional payment processing for the purchase of products or services.

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

(21) Personal data shared between a manufacturer of a tangible product and authorized third-party distributors or vendors of the product, as long as such personal data is used solely for advertising, marketing, or servicing the

product that is acquired directly through such manufacturer and such authorized third-party distributors or vendors. Such personal data may not be sold or shared unless otherwise authorized under this part.

Section 8. Section 501.705, Florida Statutes, is created to read:

501.705 Consumer rights.—

(1) A consumer is entitled to exercise the consumer rights authorized by this section at any time by submitting a request to a controller which specifies the consumer rights that the consumer wishes to exercise. With respect to the processing of personal data belonging to a known child, a parent or legal guardian of the child may exercise these rights on behalf of the child.

(2) A controller shall comply with an authenticated consumer request to exercise any of the following rights:

(a) To confirm whether a controller is processing the consumer's personal data and to access the personal data.

(b) To correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data.

(c) To delete any or all personal data provided by or obtained about the consumer.

(d) To obtain a copy of the consumer's personal data in a portable and, to the extent technically feasible, readily usable format if the data is available in a digital format.

(e) To opt out of the processing of the personal data for purposes of:

1. Targeted advertising;

2. The sale of personal data; or

3. Profiling in furtherance of a decision that produces a legal or similarly significant effect concerning a consumer.

(f) To opt out of the collection of sensitive data, including precise geolocation data, or the processing of sensitive data.

(g) To opt out of the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

(3) A device that has a voice recognition feature, a facial recognition feature, a video recording feature, an audio recording feature, or any other electronic, visual, thermal, or olfactory feature that collects data may not use those features for the purpose of surveillance by the controller, processor, or

affiliate of a controller or processor when such features are not in active use by the consumer, unless otherwise expressly authorized by the consumer.

Section 9. Section 501.706, Florida Statutes, is created to read:

501.706 Controller response to consumer requests.—

(1) Except as otherwise provided by this part, a controller shall comply with a request submitted by a consumer to exercise the consumer's rights pursuant to s. 501.705, as provided in this section.

(2) A controller shall respond to the consumer request without undue delay, which may not be later than 45 days after the date of receipt of the request. The controller may extend the response period once by an additional 15 days when reasonably necessary, taking into account the complexity and number of the consumer's requests, so long as the controller informs the consumer of the extension within the initial 45-day response period, together with the reason for the extension.

(3) If a controller cannot take action regarding the consumer's request, the controller must inform the consumer without undue delay, which may not be later than 45 days after the date of receipt of the request, of the justification for the inability to take action on the request and provide instructions on how to appeal the decision in accordance with s. 501.707. A controller is not required to comply with a consumer request submitted under s. 501.705 if the controller cannot authenticate the request. However, the controller must make a reasonable effort to request that the consumer provide additional information reasonably necessary to authenticate the consumer and the consumer's request. If a controller maintains a self-service mechanism to allow a consumer to correct certain personal data, the controller may deny the consumer's request and require the consumer to correct his or her own personal data through such mechanism.

(4) A controller must provide the consumer with notice within 60 days after the request is received that the controller has complied with the consumer's request as required in this section.

(5) A controller shall provide information or take action in response to a consumer request free of charge, at least twice annually per consumer. If a request from a consumer is manifestly unfounded, excessive, or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or may decline to act on the request. The controller bears the burden of demonstrating for purposes of this subsection that a request is manifestly unfounded, excessive, or repetitive.

(6) A controller who has obtained personal data about a consumer from a source other than the consumer is considered in compliance with a consumer's request to delete that personal data pursuant to s. 501.705(2)(c), by doing any of the following:

(a) Deleting the personal data, retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted from the business's records, and not using the retained data for any other purpose under this part.

(b) Opting the consumer out of the processing of that personal data for any purpose other than a purpose exempt under this part.

Section 10. Section 501.707, Florida Statutes, is created to read:

501.707 Appeal.—

(1) A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision under s. 501.706(3).

(2) The appeal process must be conspicuously available and similar to the process for initiating action to exercise consumer rights by submitting a request under s. 501.705.

(3) A controller shall inform the consumer in writing of any action taken or not taken in response to an appeal under this section within 60 days after the date of receipt of the appeal, including a written explanation of the reason or reasons for the decision.

Section 11. Section 501.708, Florida Statutes, is created to read:

501.708 Waiver or limitation of consumer rights prohibited.—Any provision of a contract or agreement which waives or limits in any way a consumer right described by s. 501.705, s. 501.706, or s. 501.707 is contrary to public policy and is void and unenforceable.

Section 12. Section 501.709, Florida Statutes, is created to read:

501.709 Submitting consumer requests.—

(1) A controller shall establish two or more methods to enable consumers to submit a request to exercise their consumer rights under this part. The methods must be secure, reliable, and clearly and conspicuously accessible. The methods must take all of the following into account:

(a) The ways in which consumers normally interact with the controller.

(b) The necessity for secure and reliable communications of these requests.

(c) The ability of the controller to authenticate the identity of the consumer making the request.

(2) A controller may not require a consumer to create a new account to exercise the consumer's rights under this part but may require a consumer to use an existing account.

(3) A controller shall provide a mechanism on its website for a consumer to submit a request for information required to be disclosed under this part. A controller that operates exclusively online and has a direct relationship with a consumer from whom the controller collects personal data may also provide an e-mail address for the submission of requests.

Section 13. Section 501.71, Florida Statutes, is created to read:

501.71 Controller duties.—

(1) A controller shall:

(a) Limit the collection of personal data to data that is adequate, relevant, and reasonably necessary in relation to the purposes for which it is processed, as disclosed to the consumer; and

(b) For purposes of protecting the confidentiality, integrity, and accessibility of personal data, establish, implement, and maintain reasonable administrative, technical, and physical data security practices appropriate to the volume and nature of the personal data at issue.

(2) A controller may not do any of the following:

(a) Except as otherwise provided by this part, process personal data for a purpose that is neither reasonably necessary nor compatible with the purpose for which the personal data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

(b) Process personal data in violation of state or federal laws that prohibit unlawful discrimination against consumers.

(c) Discriminate against a consumer for exercising any of the consumer rights contained in this part, including by denying goods or services, charging different prices or rates for goods or services, or providing a different level of quality of goods or services to the consumer. A controller may offer financial incentives, including payments to consumers as compensation, for processing of personal data if the consumer gives the controller prior consent that clearly describes the material terms of the financial incentive program and provided that such incentive practices are not unjust, unreasonable, coercive, or usurious in nature. The consent may be revoked by the consumer at any time.

(d) Process the sensitive data of a consumer without obtaining the consumer's consent, or, in the case of processing the sensitive data of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with the Children's Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq. for a known child under the age of 13.

(3) Paragraph (2)(c) may not be construed to require a controller to provide a product or service that requires the personal data of a consumer

which the controller does not collect or maintain or to prohibit a controller from offering a different price, rate, level, quality, or selection of goods or services to a consumer, including offering goods or services for no fee, if the consumer has exercised the consumer's right to opt out under s. 501.705(2) or the offer is related to a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or club card program.

(4) A controller that operates a search engine shall make available, in an easily accessible location on the webpage which does not require a consumer to log in or register to read, an up-to-date plain language description of the main parameters that are individually or collectively the most significant in determining ranking and the relative importance of those main parameters, including the prioritization or deprioritization of political partisanship or political ideology in search results. Algorithms are not required to be disclosed nor is any other information that, with reasonable certainty, would enable deception of or harm to consumers through the manipulation of search results.

Section 14. Section 501.711, Florida Statutes, is created to read:

501.711 Privacy notices.—

(1) A controller shall provide consumers with a reasonably accessible and clear privacy notice, updated at least annually, that includes all of the following information:

(a) The categories of personal data processed by the controller, including, if applicable, any sensitive data processed by the controller.

(b) The purpose of processing personal data.

(c) How consumers may exercise their rights under s. 501.705(2), including the process by which a consumer may appeal a controller's decision with regard to the consumer's request.

(d) If applicable, the categories of personal data that the controller shares with third parties.

(e) If applicable, the categories of third parties with whom the controller shares personal data.

(f) A description of the methods specified in s. 501.709, by which consumers can submit requests to exercise their consumer rights under this part.

(2) If a controller engages in the sale of personal data that is sensitive data, the controller must provide the following notice: "NOTICE: This website may sell your sensitive personal data." The notice must be posted in accordance with subsection (1).

(3) If a controller engages in the sale of personal data that is biometric data, the controller must provide the following notice: "NOTICE: This website may sell your biometric personal data." The notice must be posted in accordance with subsection (1).

(4) If a controller sells personal data to third parties or processes personal data for targeted advertising, the controller must clearly and conspicuously disclose that process and the manner in which a consumer may exercise the right to opt out of that process.

(5) 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.

Section 15. Section 501.712, Florida Statutes, is created to read:

501.712 Duties of processor.—

(1) A processor shall adhere to the instructions of a controller and shall assist the controller in meeting or complying with the controller's duties under this section and the requirements of this part, including the following:

(a) Assisting the controller in responding to consumer rights requests submitted pursuant to ss. 501.705 and 501.709, by using appropriate technical and organizational measures, as reasonably practicable, taking into account the nature of processing and the information available to the processor.

(b) Assisting the controller with regard to complying with the requirement relating to the security of processing personal data and to the notification of a breach of security of the processor's system under s. 501.171, taking into account the nature of processing and the information available to the processor.

(c) Providing necessary information to enable the controller to conduct and document data protection assessments under s. 501.713.

(2) A contract between a controller and a processor governs the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must include all of the following information:

(a) Clear instructions for processing data.

(b) The nature and purpose of processing.

(c) The type of data subject to processing.

(d) The duration of processing.

(e) The rights and obligations of both parties.

(f) A requirement that the processor:

1. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;

2. At the controller's direction, delete or return all personal data to the controller as requested after the provision of the service is completed, unless retention of the personal data is required by law;

3. Make available to the controller, upon reasonable request, all information in the processor's possession necessary to demonstrate the processor's compliance with this part;

4. Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor; and

5. Engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the requirements of the processor with respect to the personal data.

(3) Notwithstanding subparagraph (2)(f)4., a processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the requirements under this part using an appropriate and accepted control standard or framework and assessment procedure. The processor shall provide a report of the assessment to the controller upon request.

(4) This section may not be construed to relieve a controller or a processor from the liabilities imposed on the controller or processor by virtue of its role in the processing relationship as described by this part.

(5) A determination as to 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 on the context in which personal data is to be processed. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains in the role of a processor.

Section 16. Section 501.713, Florida Statutes, is created to read:

501.713 Data protection assessments.—

(1) A controller shall conduct and document a data protection assessment of each of the following processing activities involving personal data:

(a) The processing of personal data for purposes of targeted advertising.

(b) The sale of personal data.

(c) The processing of personal data for purposes of profiling if the profiling presents a reasonably foreseeable risk of:

1. Unfair or deceptive treatment of or unlawful disparate impact on consumers;

2. Financial, physical, or reputational injury to consumers;

3. A physical or other intrusion on the solitude or seclusion, or the private affairs or concerns, of consumers, if the intrusion would be offensive to a reasonable person; or

4. Other substantial injury to consumers.

(d) The processing of sensitive data.

(e) Any processing activities involving personal data which present a heightened risk of harm to consumers.

(2) A data protection assessment conducted under subsection (1) must do all of the following:

(a) Identify and weigh the direct or indirect benefits that may flow from the processing to the controller, the consumer, other stakeholders, and the public against the potential risks to the rights of the consumer associated with that processing, as mitigated by safeguards that can be employed by the controller to reduce such risks.

(b) Factor into the assessment:

1. The use of deidentified data;

2. The reasonable expectations of consumers;

3. The context of the processing; and

4. The relationship between the controller and the consumer whose personal data will be processed.

(3) The disclosure of a data protection assessment in compliance with a request from the Attorney General pursuant to s. 501.72 does not constitute a waiver of attorney-client privilege or work product protection with respect to the assessment and any information contained in the assessment.

(4) A single data protection assessment may address a comparable set of processing operations which include similar activities.

(5) A data protection assessment conducted by a controller for the purpose of compliance with any other law or regulation may constitute compliance with the requirements of this section if the assessment has a reasonably comparable scope and effect.

(6) This section applies only to processing activities generated on or after July 1, 2023.

Section 17. Section 501.714, Florida Statutes, is created to read:

501.714 Deidentified data, pseudonymous data, and aggregate consumer information.—

(1) A controller in possession of deidentified data shall do all of the following:

(a) Take reasonable measures to ensure that the data cannot be associated with an individual.

(b) Maintain and use the data in deidentified form. A controller may not attempt to reidentify the data, except that the controller may attempt to reidentify the data solely for the purpose of determining whether its deidentification processes satisfy the requirements of this section.

(c) Contractually obligate any recipient of the deidentified data to comply with this part.

(d) Implement business processes to prevent the inadvertent release of deidentified data.

(2) This part may not be construed to require a controller or processor to do any of the following:

(a) Reidentify deidentified data or pseudonymous data.

(b) Maintain data in an identifiable form or obtain, retain, or access any data or technology for the purpose of allowing the controller or processor to associate a consumer request with personal data.

(c) Comply with an authenticated consumer rights request under s. 501.705 if the controller:

1. Is not reasonably capable of associating the request with the personal data or it would be unreasonably burdensome for the controller to associate the request with the personal data;

2. Does not use the personal data to recognize or respond to the specific consumer who is the subject of the personal data or associate the personal data with other personal data about the same specific consumer; and

3. Does not sell the personal data to a third party or otherwise voluntarily disclose the personal data to a third party other than a processor, except as otherwise authorized by this section.

(3) The consumer rights enumerated under s. 501.705(2), and controller duties imposed under s. 501.71, do not apply to pseudonymous data or aggregate consumer information in cases in which the controller is able to demonstrate that any information necessary to identify the consumer is kept separate and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

(4) A controller that discloses pseudonymous data, deidentified data, or aggregate consumer information shall exercise reasonable oversight to monitor compliance with any contractual commitments to which the data or information is subject and shall take appropriate steps to address any breach of the contractual commitments.

Section 18. Section 501.715, Florida Statutes, is created to read:

501.715 Requirements for sensitive data.—

(1) A person who meets the requirements of s. 501.702(9)(a)1., (a)2., and (a)3. for the definition of a controller may not engage in the sale of personal data that is sensitive data without receiving prior consent from the consumer or, if the sensitive data is of a known child, without processing that data with the affirmative authorization for such processing by a known child who is between 13 and 18 years of age or in accordance with the Children's Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq. for a known child under the age of 13.

(2) A person in subsection (1) who engages in the sale of personal data that is sensitive data must provide the following notice: "NOTICE: This website may sell your sensitive personal data."

(3) A person who violates this section is subject to the penalty imposed under s. 501.72.

Section 19. Section 501.716, Florida Statutes, is created to read:

501.716 Exemptions for certain uses of consumer personal data.—

(1) This part may not be construed to restrict a controller's or processor's ability to do any of the following:

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

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

(c) Investigate, establish, exercise, prepare for, or defend legal claims.

(d) Provide a product or service specifically requested by a consumer or the parent or guardian of a child, perform a contract to which the consumer is a party, including fulfilling the terms of a written warranty, or take steps at the request of the consumer before entering into a contract.

(e) Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or of another individual and in which the processing cannot be manifestly based on another legal basis.

(f) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities, or any illegal activity.

(g) Preserve the integrity or security of systems or investigate, report, or prosecute those responsible for breaches of system security.

(h) Engage in public or peer-reviewed scientific or statistical research in the public interest which adheres to all other applicable ethics and privacy laws and is approved, monitored, and governed by an institutional review board or similar independent oversight entity that determines:

1. Whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;

2. Whether the expected benefits of the research outweigh the privacy risks; and

3. Whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including any risks associated with reidentification.

(i) Assist another controller, processor, or third party in complying with the requirements of this part.

(j) Disclose personal data disclosed when a consumer uses or directs the 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.

(k) Transfer personal data to a third party as an asset that is part of a merger, an acquisition, a bankruptcy, or other transaction in which the third party assumes control of all or part of the controller, provided that the information is used or shared in a manner consistent with this part. If a third party materially alters how it uses or shares the personal data of a consumer in a manner that is materially inconsistent with the commitments or promises made at the time of collection, it must 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 part.

(2) This part may not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this state as part of a privileged communication.

(3) This part may not be construed as imposing a requirement on controllers and processors which adversely affects the rights or freedoms of any person, including the right of free speech.

(4) This part may not be construed as requiring a controller, processor, third party, or consumer to disclose a trade secret.

Section 20. Section 501.717, Florida Statutes, is created to read:

501.717 Collection, use, or retention of data for certain purposes.—

(1) The requirements imposed on controllers and processors under this part may not restrict a controller's or processor's ability to collect, use, or retain data to do any of the following:

(a) Conduct internal research to develop, improve, or repair products, services, or technology.

(b) Effect a product recall.

(c) Identify and repair technical errors that impair existing or intended functionality.

(d) Perform internal operations that are:

1. Reasonably aligned with the expectations of the consumer;

2. Reasonably anticipated based on the consumer's existing relationship with the controller; or

3. Otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

(2) A requirement imposed on a controller or processor under this part does not apply if compliance with the requirement by the controller or processor, as applicable, would violate an evidentiary privilege under the laws of this state.

Section 21. Section 501.718, Florida Statutes, is created to read:

501.718 Disclosure of personal data to third-party controller or processor.—

(1) A controller or processor that discloses personal data to a third-party controller or processor in compliance with the requirements of this part does not violate this part if the third-party controller or processor that receives and processes that personal data violates this part, provided that, at the time of the data's disclosure, the disclosing controller or processor could not have reasonably known that the recipient intended to commit a violation.

(2) A third-party controller or processor receiving personal data from a controller or processor in compliance with the requirements of this part may not be held liable for violations of this part committed by the controller or processor from which the third-party controller or processor receives the personal data.

Section 22. Section 501.719, Florida Statutes, is created to read:

501.719 Processing of certain personal data by controller or other person.—

(1) Personal data processed by a controller pursuant to ss. 501.716, 501.717, and 501.718 may not be processed for any purpose other than those specified in those sections. Personal data processed by a controller pursuant to ss. 501.716, 501.717, and 501.718 may be processed to the extent that the processing of the data is:

(a) Reasonably necessary and proportionate to the purposes specified in ss. 501.716, 501.717, and 501.718;

(b) Adequate, relevant, and limited to what is necessary in relation to the purposes specified in ss. 501.716, 501.717, and 501.718; and

(c) Done to assist another controller, processor, or third party with any of the purposes specified in s. 501.716, s. 501.717, or s. 501.718.

(2) A controller or processor that collects, uses, or retains personal data for the purposes specified in s. 501.717(1) must take into account the nature and purpose of such collection, use, or retention. Such personal data is subject to reasonable administrative, technical, and physical measures to protect its confidentiality, integrity, and accessibility and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use, or retention of personal data.

(3) A controller or processor shall adopt and implement a retention schedule that prohibits the use or retention of personal data 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 2 years after the consumer's last interaction with the controller or processor. This subsection does not apply to personal data reasonably used or retained to do any of the following:

(a) 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.

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

(c) 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.

(4) A controller or processor that processes personal data pursuant to ss. 501.716, 501.717, and 501.718 bears the burden of demonstrating that the processing of the personal data qualifies for the exemption and complies with the requirements of this section.

Section 23. Section 501.72, Florida Statutes, is created to read:

501.72 Enforcement and implementation by the Department of Legal Affairs.—

(1) A violation of this part is an unfair and deceptive trade practice actionable under part II of this chapter solely by the Department of Legal Affairs. If the department has reason to believe that a person is in violation of this section, the department may, as the enforcing authority, bring an action against such person for an unfair or deceptive act or practice. For the purpose of bringing an action pursuant to this section, ss. 501.211 and 501.212 do not apply. In addition to other remedies under part II of this chapter, the department may collect a civil penalty of up to $50,000 per violation. Civil penalties may be tripled for any of the following violations:

(a) A violation involving a Florida consumer who is a known child. A controller that willfully disregards the consumer's age is deemed to have actual knowledge of the consumer's age.

(b) Failure to delete or correct the consumer's personal data pursuant to this section after receiving an authenticated consumer request or directions from a controller to delete or correct such personal data, unless an exception to the requirements to delete or correct such personal data under this section applies.

(c) Continuing to sell or share the consumer's personal data after the consumer chooses to opt out under this part.

(2) After the department has notified a person in writing of an alleged violation, the department may grant a 45-day period to cure the alleged violation and issue a letter of guidance. The 45-day cure period does not apply to an alleged violation of paragraph (1)(a). 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 in determining whether to grant 45 calendar days to cure and the issuance of a letter of guidance. If the alleged violation is cured to the satisfaction of the department and proof of such cure is provided to the department, the department may not bring an action for the alleged violation but in its discretion may issue a letter of guidance that indicates that the person will not be offered a 45-day cure period for any future violations. If the person

fails to cure the alleged violation within 45 calendar days, the department may bring an action against such person for the alleged violation.

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

(4) By February 1 of each year, the department shall make a report publicly available on the department's website describing any actions taken by the department to enforce this section. The report must include statistics and relevant information detailing all of the following:

(a) The number of complaints received and the categories or types of violations alleged by the complainant.

(b) The number and type of enforcement actions taken and the outcomes of such actions, including the amount of penalties issued and collected.

(c) The number of complaints resolved without the need for litigation.

(d) For the report due February 1, 2024, the status of the development and implementation of rules to implement this section.

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

(6) The department may collaborate and cooperate with other enforcement authorities of the Federal Government or other state governments concerning consumer data privacy issues and consumer data privacy investigations if such enforcement authorities have restrictions governing confidentiality at least as stringent as the restrictions provided in this section.

(7) Liability for a tort, contract claim, or consumer protection claim unrelated to an action brought under this section does not arise solely from the failure of a person to comply with this part.

(8) This part does not establish a private cause of action.

(9) The department may employ or use the legal services of outside counsel and the investigative services of outside personnel to fulfill the obligations of this section.

(10) For purposes of bringing an action pursuant to this section, any person who meets the definition of controller as defined in this part who collects, shares, or sells the personal data of Florida consumers is considered to be engaged in both 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 24. Section 501.721, Florida Statutes, is created to read:

501.721 Preemption.—This part 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 data by a controller or processor. The regulation of the collection, processing, sharing, or sale of consumer personal data by a controller or processor is preempted to the state.

Section 25. 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 data as defined in s. 501.702; or

(VII) Any information regarding an individual's geolocation.

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

16.53 Legal Affairs Revolving Trust Fund.—

(1) There is created in the State Treasury the Legal Affairs Revolving Trust Fund, from which the Legislature may appropriate funds for the purpose of funding investigation, prosecution, and enforcement by the Attorney General of the provisions of the Racketeer Influenced and Corrupt Organization Act, the Florida Deceptive and Unfair Trade Practices Act, the Florida False Claims Act, ~~or~~ state or federal antitrust laws, s. 501.1735, or part V of chapter 501.

(8) All moneys recovered by the Attorney General for attorney fees, costs, and penalties in an action for a violation of s. 501.1735 or part V of chapter 501 must be deposited in the fund.

Section 27. Except as otherwise expressly provided in this act and except for this section, which shall take effect upon this act becoming a law, this act shall take effect July 1, 2024.

Approved by the Governor June 6, 2023.

Filed in Office Secretary of State June 6, 2023.