A bill to be entitled
An act relating to consumer data privacy; amending s. 501.171, F.S.; revising the definition of "personal information" to include additional specified information to data breach reporting requirements; creating s. 501.173, F.S.; providing definitions; requiring businesses 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 businesses from collecting additional categories of personal information or using personal information for additional purposes without notifying the consumer; requiring businesses that collect personal information to implement reasonable security procedures and practices to protect the information; authorizing consumers to request businesses to disclose the specific personal information the business has collected about the consumer; requiring businesses to make available two or more methods for consumers to request their personal information;
requiring businesses 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 businesses to delete or correct personal information the businesses have collected about the consumers; providing exceptions; specifying requirements for businesses to comply with deletion or correction requests; authorizing consumers to opt out of third-party disclosure of personal information collected by a business; prohibiting businesses from selling or disclosing the personal information of consumers younger than a certain age, except under certain circumstances; prohibiting businesses from selling or sharing a consumer's information if the consumer has opted out of such disclosure; prohibiting businesses from taking certain actions to retaliate against consumers who exercise certain rights; providing exceptions; providing applicability; providing that a contract or agreement that waives or limits certain consumer rights is void and unenforceable; providing a private right of action for consumers whose nonencrypted and nonredacted personal information or
e-mail addresses are subject to unauthorized access; providing civil remedies; authorizing the Department of Legal Affairs to bring a civil action for intentional or unintentional violations and to adopt rules; providing that businesses must have a specified timeframe to cure any violations; providing an effective date.

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

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

501.171 Security of confidential personal information.—

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

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

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

(I) A social security number;

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

(III) A financial account number or credit or debit card
number, in combination with any required security code, access
code, or password that is necessary to permit access to an
individual's financial account;
   (IV) Any information regarding an individual's medical
history, mental or physical condition, or medical treatment or
diagnosis by a health care professional; or
   (V) An individual's health insurance policy number or
subscriber identification number and any unique identifier used
by a health insurer to identify the individual.
   b. A user name or e-mail address, in combination with a
password or security question and answer that would permit
access to an online account.
   c. An individual's biometric information as defined in s.
501.173(1).

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

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

501.173 Consumer data privacy.—
(1) DEFINITIONS.—As used in this section, the term:
(a) "Aggregate consumer information" means information that relates to a group or category of consumers, from which the identity of an individual consumer has been removed and is not reasonably capable of being directly or indirectly associated or linked with, any consumer or household, including via a device. The term does not include one or more individual consumer records that have been deidentified.

(b) "Biometric information" means an individual's physiological, biological, or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. The term includes, but is not limited to, imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information.

(c) "Business" 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 one or more of the following thresholds:

   (I) Has global annual gross revenues in excess of $25 million, as adjusted in January of every odd-numbered year to reflect any increase in the Consumer Price Index.

   (II) Annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 50,000 or more consumers, households, or devices.

   (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 business and that shares common branding with the business. As used in this subparagraph, the term:

   a. "Control" means:

      (I) Ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business;

      (II) Control in any manner over the election of a majority of the directors, or of individuals exercising similar
functions; or

(III) The power to exercise a controlling influence over

the management of a company.

b. "Common branding" means a shared name, servicemark, or

trademark.

d. "Business purpose" means the use of personal

information for the operational purpose of a business or service

provider, or other notified purposes, provided that the use of

personal information is reasonably necessary and proportionate

to achieve the operational purpose for which the personal

information was collected or processed or for another

operational purpose that is compatible with the context in which

the personal information was collected. The term includes:

1. Auditing relating to a current interaction with a

consumer and concurrent transactions, including, but not limited

to, counting ad impressions to unique visitors, verifying

positioning and quality of ad impressions, and auditing

compliance with this specification and other standards.

2. Detecting security incidents; protecting against

malicious, deceptive, fraudulent, or illegal activity; and

prosecuting those responsible for that activity.

3. Debugging to identify and repair errors that impair

existing intended functionality.

4. Short-term, transient use, provided that the personal

information is not disclosed to another third party and is not
used to build a profile about a consumer or otherwise alter an individual consumer's experience outside the current interaction, including, but not limited to, the contextual customization of ads shown as part of the same interaction.

5. Performing services on behalf of the business or service provider, including maintaining or servicing accounts, providing customer service, processing or fulfilling orders and transactions, verifying customer information, processing payments, providing financing, providing analytic services, or providing similar services on behalf of the business or service provider.

6. Undertaking internal research for technological development and demonstration.

7. Undertaking activities to verify or maintain the quality or safety of a service or device that is owned, manufactured, manufactured for, or controlled by the business, and to improve, upgrade, or enhance the service or device that is owned, manufactured, manufactured for, or controlled by the business.

(e) "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.

(f) "Commercial purposes" means to advance the commercial
or economic interests of a person, such as inducing another
person to buy, rent, lease, join, subscribe to, provide, or
exchange products, goods, property, information, or services, or
directly or indirectly enabling or effecting a commercial
transaction.

(g) "Consumer" means a natural person who resides in or is
domiciled in this state, however identified, including by any
unique identifier, and who is:

1. In this state for other than a temporary or transitory
   purpose; or
2. Domiciled in this state but resides outside this state
   for a temporary or transitory purpose.

(h) "Deidentified" means information that does not
reasonably identify, relate to, or describe a particular
consumer, or is not reasonably capable of being directly or
indirectly associated or linked with a particular consumer,
provided that a business that uses deidentified information:

1. Implements technical safeguards that prohibit
   reidentification of the consumer to whom the information may
   pertain.
2. Implements business processes that specifically
   prohibit reidentification of the information.
3. Implements business processes to prevent inadvertent
   release of deidentified information.
4. Does not attempt to reidentify the information.
(i) "Department" means the Department of Legal Affairs.

(j) "Health insurance information" means a consumer's insurance policy number or subscriber identification number, or any unique identifier used by a health insurer to identify the consumer, or any information in the consumer's application and claims history, including any appeals records, if the information is reasonably capable of being directly or indirectly associated or linked with a consumer or household, including via a device, by a business or service provider.

(k) "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 (9), including, but not limited to, before downloading the application.

(l) "Person" means an individual, proprietorship, firm, partnership, joint venture, syndicate, business trust, company, corporation, limited liability company, association, committee, and any other organization or group of persons acting in concert.

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

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

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

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

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

   d. Commercial information, including records of personal
property, products or services purchased, obtained, or
considered, or other purchasing or consuming histories or
tendencies.

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

g. Geolocation data.

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

i. Professional or employment-related information.

j. Education information that is not publicly available,
personally identifiable information as defined in the Family
Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34
C.F.R. part 99.

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

2. The term does not include consumer information that is:
a. Publicly and lawfully made available from federal,
state, or local government records.

b. Deidentified or aggregate consumer information.

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

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

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

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

1. Compatible with the business purpose for which the personal information was collected.

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

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

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

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

6. Protected from any reidentification attempts.

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

8. Subjected by the business conducting the research to
additional security controls that limit access to the research
data to only those individuals in a business necessary to carry
out the research purpose.

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

(s) "Service" means work or labor furnished in connection
with the sale or repair of goods.
(t) "Service provider" 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 business and to which the business discloses a consumer's personal information for a business purpose 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 business, or as otherwise permitted by this section, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract with the business.

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

1. Allowing a third party to use or advertise 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 business and a third party for advertising for the benefit of a business.

(v) "Third party" means a person who is not any of the

CODING: Words stricken are deletions; words underlined are additions.
following:

1. A business that collects personal information from consumers under this section.

2. A person to whom the business discloses personal information about consumers for a business purpose pursuant to a written contract.

(w) "Unique identifier" means a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family, over time and across different services, including, but not limited to, a device identifier; an Internet Protocol address; cookies, beacons, pixel tags, mobile ad identifiers, or similar technology; customer number, unique pseudonym, or user alias; telephone numbers, or other forms of persistent or probabilistic identifiers which can be used to identify a particular consumer or device. As used in this paragraph, the term "family" means a custodial parent or guardian and any minor children of whom the parent or guardian has custody, or a household.

(x) "Verifiable consumer request" means a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify pursuant to rules adopted by the department to be the consumer about whom the business has collected personal information. A business is not obligated to
provide information to the consumer if the business cannot verify that the consumer making the request is the consumer about whom the business has collected information or is a person authorized by the consumer to act on the consumer's behalf.

(2) PRIVACY POLICY FOR PERSONAL INFORMATION.—

(a) A business that collects personal information about consumers shall maintain an online privacy policy, make such policy available on its Internet website, and update the information at least once every 12 months. The online privacy policy must include the following information:

1. Any Florida-specific consumer privacy rights.

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

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

4. Of the categories identified in subparagraph 2., a list that identifies which categories of personal information the business discloses or shares or has disclosed or shared about consumers for a business purpose. If the business does not disclose or share personal information for a business purpose, the business shall disclose that fact.

5. The right to opt-out of the sale or sharing to third
parties and the ability to request deletion or correction of certain personal information.

(b) A consumer has the right to request that a business that collects personal information disclose to the consumer the categories and specific pieces of personal information the business collects from or about consumers.

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

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

(e) A business shall provide the information specified in paragraph (b) to a consumer only upon receipt of a verifiable consumer request.

(f) A business shall provide and follow a retention schedule that prohibits the use and retention of personal information after satisfaction of the initial purpose for collecting or obtaining such information, or after the duration of a contract, or 1 year after the consumer's last interaction with the business, whichever occurs first. This paragraph does not apply to biometric information used for ticketing purposes.
and does not apply if such information is only kept for the time related to the duration of the ticketed event.

(3) CONSUMER RIGHT TO REQUEST COPY OF PERSONAL DATA COLLECTED.—

(a) A consumer has the right to request that a business that collects personal information about the consumer disclose the personal information that has been collected by the business.

(b) A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information must be in a portable and, to the extent technically feasible, readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but may not be required to provide personal information to a consumer more than twice in a 12-month period.

(c) A business shall disclose the following to the consumer:

1. The specific pieces of personal information it has collected about the consumer.

2. The categories and sources from which it collected the
consumer's personal information.

3. The business or commercial purpose for collecting or selling the consumer's personal information.

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

(d) A business that collects personal information about a consumer shall disclose the information specified in paragraph (a) to the consumer upon receipt of a verifiable consumer request from the consumer.

(e) This subsection does not require a business to do the following:

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

2. Reidentify or otherwise link any data that, in the ordinary course of business, is not maintained in a manner that would be considered personal information.

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

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

(b) A business that receives a verifiable consumer request from a consumer to delete the consumer's personal information
shall delete the consumer's personal information from its
records and direct any service providers to delete the
consumer's personal information from their records.

(c) A business or a service provider may not be required
to comply with a consumer's request to delete the consumer's
personal information if it is necessary for the business or
service provider to maintain the consumer's personal information
to do any of the following:

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

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

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

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

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

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

7. Enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business.

8. Comply with a legal obligation.

9. Otherwise internally use the consumer's personal information in a lawful manner that is compatible with the context in which the consumer provided the information.

(d) A consumer has the right to request a business that maintains inaccurate personal information about the consumer to correct the inaccurate personal information, taking into account the nature of the personal information and the purposes of the processing of the personal information. A business 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.

(5) RIGHT TO REQUEST PERSONAL DATA SOLD OR SHARED.—

(a) A consumer has the right to request that a business that sells or shares personal information about the consumer, or discloses such information for a business purpose, to disclose to the consumer:

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

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

3. The categories of personal information about the
consumer that the business disclosed for a business purpose.

(b) A business that sells or shares personal information
about consumers or discloses such information for a business
purpose shall disclose the information specified in paragraph
(a) to the consumer upon receipt of a verifiable consumer
request from the consumer.

(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 business unless the consumer has received
explicit notice and is provided an opportunity to opt-out.

6. RIGHT TO OPT-OUT OF THE SALE OR SHARING OF PERSONAL
INFORMATION TO THIRD PARTIES.—

(a) A consumer has the right at any time to direct a
business that sells or shares personal information about the
consumer to third parties to not sell or share the consumer's
personal information. This right may be referred to as the right
to opt-out.

(b) A business that sells or shares personal information
to third parties shall provide notice to consumers that this
information may be sold and shared and that consumers have the
right to opt-out of the sale or sharing of their personal
information.

(c) Notwithstanding paragraph (a), a business may not sell or share the personal information of a consumer if the business has actual knowledge that the consumer is not 16 years of age or older, unless the consumer, in the case of consumers between 13 and 15 years of age, or the consumer's parent or guardian, in the case of consumers who are 12 years of age or younger, has affirmatively authorized the sale or sharing of the consumer's personal information. A business that willfully disregards the consumer's age is deemed to have had actual knowledge of the consumer's age. This right may be referred to as the right to opt-in.

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

(e) A business does not sell personal information when:
   1. A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that
disclosure would be consistent with the provisions of this section. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party.

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

3. The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met:
   a. The business has provided notice that the personal information of the consumer is being used or shared in its terms and conditions consistent with subsection (9).
   b. The service provider does not further collect, sell, share, or use the personal information of the consumer except as necessary to perform the business purpose.

4. The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with subsections...
(3) and (5). If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice must be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with this subsection.

(f) A business does not share personal information when:

1. A consumer uses or directs the business to intentionally disclose personal information or intentionally interact with one or more third parties.

2. The business uses or shares an identifier for a consumer who has opted-out of sharing the consumer's personal information for the purposes of alerting persons that the consumer has opted-out of sharing the consumer's personal information.

(7) DISCRIMINATION AGAINST CONSUMERS WHO EXERCISE THEIR RIGHTS.—

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

a. Denying goods or services to the consumer.

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

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

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

2. This paragraph does not prohibit a business from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, if that difference is reasonably related to the value provided to the business by the consumer's data.

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

2. A business may offer a different price, rate, level, or quality of goods or services to the consumer if the price or difference is directly related to the value provided to the business by the consumer's personal information.

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

4. A business may enter a consumer into a financial incentive program only if the consumer gives the business prior consent that clearly describes the material terms of the financial incentive program. The consent may be revoked by the consumer at any time.
5. A business may not use financial incentive practices that are unjust, unreasonable, coercive, or usurious in nature.

(8) REQUESTS FOR PERSONAL INFORMATION.—

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

(b) The business shall deliver the information required or act on the request in subsections (3) through (6) to a consumer free of charge within 45 days after receiving a verifiable consumer request. The response period may be extended once by 30 additional days when reasonably necessary, taking into account the complexity of the consumer's requests, provided the business informs the consumer of any such extension within the initial 45-day response period along with the reason for the extension. The information must be delivered in a readily usable format that allows the consumer to transmit the information from one entity to another entity without hindrance.

(c) If a third party assumes control of all or part of a business and acquires a consumer's personal information as part of the transfer, and the third party materially alters how it
uses a consumer's personal information or shares the information in a manner that is materially inconsistent with the promises made at the time of collection, the third party must provide prior notice of the new or changed practice to the customer. The notice must be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices.

(d) Any contract between a business and a service provider must prohibit the service provider from:

1. Selling or sharing the personal information;
2. Retaining, using, or disclosing the personal information for any purpose other than for the business purposes specified in the contract for the business, including retaining, using, or disclosing the personal information for a commercial purpose other than the business purposes specified in the contract with the business;
3. Retaining, using, or disclosing the information outside of the direct business relationship between the service provider and the business; or
4. Combining the personal information that the service provider receives from or on behalf of the business with personal information that it receives from or on behalf of another person or entity or that the service provider collects from its own interaction with the consumer, provided that the service provider may combine personal information to perform any business purpose.
(e) Any contract between a business and a third party must prohibit the third party that receives a consumer's personal information from the following:

1. Selling or sharing the personal information.
2. Retaining, using, or disclosing the personal information for any purpose other than the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
3. Retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract, including retaining, using, or disclosing the personal information for a commercial purpose other than providing the services specified in the contract.
4. Retaining, using, or disclosing the information outside of the direct business relationship between the person and the business.

The contract must include a certification made by the person or entity receiving the personal information stating that the person or entity understands and will comply with the restrictions under this paragraph.

(f) Any contract between a business and a third party or
between a business and a service provider for receiving personal information must include a provision that any contract between a third party and any subcontractor or between a service provider and any subcontractor must require the subcontractor to meet the obligations of the third party or service provider with respect to personal information.

(g) A third party or service provider or any subcontractor thereof who violates any of the restrictions imposed upon it under this section is liable for any violations. A business that discloses personal information to a third party or service provider in compliance with this section is not liable if the person receiving the personal information uses it in violation of the restrictions under this section, provided that at the time of disclosing the personal information, the business does not have actual knowledge or reason to believe that the person intends to commit such a violation.

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

(a) A business shall, in a form that is reasonably accessible to consumers:

1. Provide a clear and conspicuous link on the business'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 business may
not require a consumer to create an account in order to direct
the business not to sell the consumer's personal information.

2. Include a description of a consumer's rights along with
a separate link to the "Do Not Sell or Share My Personal
Information" Internet webpage in:
   a. Its online privacy policy or policies.
   b. Any Florida-specific consumer privacy rights.

3. Ensure that all individuals responsible for handling
consumer inquiries about the business's privacy practices or the
business's compliance with this section are informed of all
requirements in subsection (6) and this subsection and how to
direct consumers to exercise their rights subsection (6) and
this subsection.

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

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

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

Page 32 of 37

CODING: Words **stricken** are deletions; words *underlined* are additions.
opt-out request.

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

(c) A consumer may authorize another person to opt-out of the sale or sharing of the consumer's personal information on the consumer's behalf, and a business shall comply with an opt-out request received from a person authorized by the consumer to act on the consumer's behalf, pursuant to rules adopted by the department.

(10) EXCEPTIONS.—

(a) This section does not restrict any business' or third party's ability to do any of the following:

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

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

3. Cooperate with law enforcement agencies concerning conduct or activity that the business, service provider, or
third party reasonably and in good faith believes may violate federal, state, or local law.

4. Exercise legal rights or privileges.
5. Collect, use, retain, sell, or disclose deidentified personal information or aggregate consumer information. If a business uses deidentified information, the business shall:
   a. Implement technical safeguards that prohibit reidentification of the consumer to whom the information may pertain;
   b. Implement business processes that specifically prohibit reidentification of the information;
   c. Implement business processes to prevent inadvertent release of deidentified information; and
   d. Not attempt to reidentify the information.

(b) This section does not apply to:
1. A business that collects or discloses its employees' personal information, so long as the business is collecting or disclosing such information within the scope of its role as an employer.
2. Health information that is collected by 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.
3. A covered entity governed by the privacy, security, and
breach notification rules issues by the United States Department of Health and Human Services in 45 C.F.R. parts 160 and 164, to the extent the provider or covered entity maintains patient information in the same manner as medical information or protected health information as described in subparagraph 2.

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

5. Sale or sharing of personal information to or from a consumer reporting agency if that information is to be reported in or used to generate a consumer report as defined by 15 U.S.C. s. 1681(a), and if use of that information is limited by the federal Fair Credit Reporting Act, 15 U.S.C. s. 1681 et seq.

6. 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.

7. 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.

8. Education information covered by the Family Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34 C.F.R. part
9. Information collected as part of public or peer-reviewed scientific or statistical research in the public interest.

(11) CONTRACTS.—Any provision of a contract or agreement of any kind that waives or limits in any way a consumer's rights under this section, including, but not limited to, any right to a remedy or means of enforcement, is deemed contrary to public policy and is void and unenforceable. This section does not prevent a consumer from declining to request information from a business, declining to opt-out of a business's sale or sharing of the consumer's personal information, or authorizing a business to sell or share the consumer's personal information after previously opting out. This subsection only applies to contracts entered into after January 1, 2022.

(12) PRIVATE CAUSE OF ACTION.—A consumer whose nonencrypted and nonredacted personal information or e-mail address, in combination with a password or security question and answer that would allow access to the account, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of a business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may bring a civil action for any of the following:
(a) Damages in an amount not less than $100 and not
greater than $750 per consumer per incident or actual damages,
whichever is greater.

(b) Injunctive or declaratory relief, as the court deems
proper.

(13) ENFORCEMENT AND IMPLEMENTATION.—

(a) If the department has reason to believe that any
business, service provider, or other person or entity is in
violation of this section and that proceedings would be in the
public interest, the department may bring an action against such
business, service provider, or other person or entity and may
seek a civil penalty of not more than $2,500 for each
unintentional violation or $7,500 for each intentional
violation. Such fines may be tripled if the violation involves a
consumer who is 16 years of age or younger.

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

(c) A business may be found to be in violation of this
section if it fails to cure any alleged violation within 30 days
after being notified in writing by the department of the alleged
noncompliance.

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