

1 A bill to be entitled
2 An act relating to consumer data privacy; creating s.
3 501.173, F.S.; providing applicability; providing
4 definitions; requiring controllers that collect a
5 consumer's personal data to disclose certain
6 information regarding data collection and selling
7 practices to the consumer at or before the point of
8 collection; specifying that such information may be
9 provided through a general privacy policy or through a
10 notice informing the consumer that additional specific
11 information will be provided upon a certain request;
12 prohibiting controllers from collecting additional
13 categories of personal information or using personal
14 information for additional purposes without notifying
15 the consumer; requiring controllers that collect
16 personal information to implement reasonable security
17 procedures and practices to protect the information;
18 authorizing consumers to request controllers to
19 disclose the specific personal information the
20 controller has collected about the consumer; requiring
21 controllers to make available two or more methods for
22 consumers to request their personal information;
23 requiring controllers to provide such information free
24 of charge within a certain timeframe and in a certain
25 format upon receiving a verifiable consumer request;

26 specifying requirements for third parties with respect
27 to consumer information acquired or used; providing
28 construction; authorizing consumers to request
29 controllers to delete or correct personal information
30 the controllers have collected about the consumers;
31 providing exceptions; specifying requirements for
32 controllers to comply with deletion or correction
33 requests; authorizing consumers to opt out of third-
34 party disclosure of personal information collected by
35 a controller; prohibiting controllers from selling or
36 disclosing the personal information of consumers
37 younger than a certain age, except under certain
38 circumstances; prohibiting controllers from selling or
39 sharing a consumer's information if the consumer has
40 opted out of such disclosure; prohibiting controllers
41 from taking certain actions to retaliate against
42 consumers who exercise certain rights; providing
43 applicability; providing that a contract or agreement
44 that waives or limits certain consumer rights is void
45 and unenforceable; providing for civil actions and a
46 private right of action for consumers under certain
47 circumstances; providing civil remedies; authorizing
48 the Department of Legal Affairs to bring an action
49 under the Florida Unfair or Deceptive Trade Practices
50 Act and to adopt rules; requiring the department to

51 submit an annual report to the Legislature; providing
 52 report requirements; providing that controllers must
 53 have a specified timeframe to cure any violations;
 54 providing jurisdiction; declaring that the act is
 55 matter of statewide concern; preempting the
 56 collection, processing, sharing, and sale of consumer
 57 personal information to the state; amending s.
 58 501.171, F.S.; revising the definition of "personal
 59 information"; providing an effective date.

60
 61 Be It Enacted by the Legislature of the State of Florida:

62
 63 Section 1. Section 501.173, Florida Statutes, is created
 64 to read:

65 501.173 Consumer data privacy.-

66 (1) APPLICABILITY.-This section does not apply to:

67 (a) Personal information collected and transmitted that is
 68 necessary for the sole purpose of sharing such personal
 69 information with a financial service provider to facilitate
 70 short term, transactional payment processing for the purchase of
 71 products or services.

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

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

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

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

83 (f) Exercising legal rights or privileges.

84 (g) Personal information used or collected by a controller
 85 or processor pursuant to a written contract between the
 86 controller and processor that complies with the requirements of
 87 this section.

88 (h) Personal information used by a controller or processor
 89 to advertise or market products or services that are produced or
 90 offered directly by the controller or processor. Such
 91 information may not be sold, shared, or disclosed to another
 92 person unless otherwise authorized under this section.

93 (i) Personal information of a person acting in the role of
 94 a job applicant, employee, owner, director, officer, contractor,
 95 volunteer, or intern of a controller, that is collected by a
 96 controller, to the extent the personal information is collected
 97 and used solely within the context of the person's role or
 98 former role with the controller.

99 (j) Protected health information for purposes of the
 100 federal Health Insurance Portability and Accountability Act of

101 1996 and related regulations, and patient identifying
102 information for purposes of 42 C.F.R. part 2, established
103 pursuant to 42 U.S.C. s. 290dd-2.

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

117 (l) Identifiable private information collected for
118 purposes of research as defined in 45 C.F.R. s. 164.501
119 conducted in accordance with the Federal Policy for the
120 Protection of Human Subjects for purposes of 45 C.F.R. part 46,
121 the good clinical practice guidelines issued by the
122 International Council for Harmonisation of Technical
123 Requirements for Pharmaceuticals for Human Use, or the
124 Protection for Human Subjects for purposes of 21 C.F.R. parts 50
125 and 56, or personal information that is used or shared in

126 research conducted in accordance with one or more of these
127 standards.

128 (m) Information and documents created for purposes of the
129 federal Health Care Quality Improvement Act of 1986 and related
130 regulations, or patient safety work product for purposes of 42
131 C.F.R. part 3, established pursuant to 42 U.S.C. s. 299b-21
132 through 299b-26.

133 (n) Information that is deidentified in accordance with 45
134 C.F.R. part 164 and derived from individually identifiable
135 health information as described in the Health Insurance
136 Portability and Accountability Act of 1996, or identifiable
137 personal information, consistent with the Federal Policy for the
138 Protection of Human Subjects or the human subject protection
139 requirements of the United States Food and Drug Administration.

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

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

145 (q) Nonpublic personal information collected, processed,
146 sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, 15
147 U.S.C. s. 6801 et seq., and implementing regulations.

148 (r) A financial institution as defined in the Gramm-Leach-
149 Bliley Act, 15 U.S.C. s. 6801 et seq., to the extent the
150 financial institution maintains personal information in the same

HB9

2022

151 manner as nonpublic personal information as described in
152 paragraph (q), and as long as such financial institution does
153 not use personal information for targeted advertising with third
154 parties and does not sell or share personal information to a
155 third party unless such sale or sharing is covered by an
156 exception under this section.

157 (s) Personal information collected, processed, sold, or
158 disclosed pursuant to the federal Driver's Privacy Protection
159 Act of 1994, 18 U.S.C. s. 2721 et seq.

160 (t) Education information covered by the Family
161 Educational Rights and Privacy Act, 20 U.S.C. s. 1232(g) and 34
162 C.F.R. part 99.

163 (u) Information collected as part of public or peer-
164 reviewed scientific or statistical research in the public
165 interest and that adheres to all other applicable ethics and
166 privacy laws, if the consumer has provided informed consent.
167 Research with personal information must be subjected by the
168 controller conducting the research to additional security
169 controls that limit access to the research data to only those
170 individuals necessary to carry out the research purpose and
171 subsequently deidentified.

172 (v) Personal information disclosed for the purpose of
173 responding to an alert of a present risk of harm to a person or
174 property, detecting security incidents, protecting against
175 malicious, deceptive, fraudulent, or illegal activity, or

HB9

2022

176 prosecuting those responsible for that activity.

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

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

191 (y) Personal information transferred by a controller to a
192 third party as an asset that is part of a merger, acquisition,
193 bankruptcy, or other transaction in which the third party
194 assumes control of all or part of the controller, provided that
195 information is used or shared consistently with this section. If
196 a third party materially alters how it uses or shares the
197 personal information of a consumer in a manner that is
198 materially inconsistent with the commitments or promises made at
199 the time of collection, it shall provide prior notice of the new
200 or changed practice to the consumer. The notice must be

201 sufficiently prominent and robust to ensure that consumers can
 202 easily exercise choices consistent with this section.

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

204 (a) "Aggregate consumer information" means information
 205 that relates to a group or category of consumers, from which the
 206 identity of an individual consumer has been removed and is not
 207 reasonably capable of being directly or indirectly associated or
 208 linked with, any consumer, household, or device. The term does
 209 not include personal information that has been deidentified.

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

222 (c) "Collect" means to buy, rent, gather, obtain, receive,
 223 or access any personal information pertaining to a consumer by
 224 any means. The term includes, but is not limited to, actively or
 225 passively receiving information from the consumer or by

226 observing the consumer's behavior or actions.

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

233 (e) "Controller" means:

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

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

239 b. Does business in this state;

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

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

245 e. Satisfies at least two of the following thresholds:

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

249 (II) Annually buys, receives, sells, or shares the
250 personal information of 50,000 or more consumers, households, or

251 devices for the purpose of targeted advertising in conjunction
 252 with third parties or for a purpose that is not listed under
 253 subsection (1).

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

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

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

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

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

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

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

274 2. Maintains and uses the information in deidentified form
 275 and not to attempt to reidentify the information, except that

276 the controller may attempt to reidentify the information solely
277 for the purpose of determining whether its deidentification
278 processes satisfy the requirements of this paragraph; and

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

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

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

286 (i) "Homepage" means the introductory page of an Internet
287 website and any Internet webpage where personal information is
288 collected. In the case of a mobile application, the homepage is
289 the application's platform page or download page, a link within
290 the application, such as the "About" or "Information"
291 application configurations, or settings page, and any other
292 location that allows consumers to review the notice required by
293 subsection (7), including, but not limited to, before
294 downloading the application.

295 (j) "Household" means a natural person or a group of
296 people in this state who reside at the same address, share a
297 common device or the same service provided by a controller, and
298 are identified by a controller as sharing the same group account
299 or unique identifier.

300 (k) "Personal information" means information that is

301 linked or reasonably linkable to an identified or identifiable
302 consumer or household, including biometric information and
303 unique identifiers to the consumer. The term does not include
304 consumer information that is:

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

310 2. Deidentified or aggregate consumer information.

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

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

315 b. By a widely distributed media source.

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

320 (l) "Processing" means any operation or set of operations
321 that are performed on personal information or on sets of
322 personal information, whether or not by automated means.

323 (m) "Processor" means a sole proprietorship, partnership,
324 limited liability company, corporation, association, or other
325 legal entity that is organized or operated for the profit or

326 financial benefit of its shareholders or other owners, that
327 processes information on behalf of a controller and to which the
328 controller discloses a consumer's personal information pursuant
329 to a written contract, provided that the contract prohibits the
330 entity receiving the information from retaining, using, or
331 disclosing the personal information for any purpose other than
332 for the specific purpose of performing the services specified in
333 the contract for the controller, or as otherwise permitted by
334 this section.

335 (n) "Sell" means to sell, rent, release, disclose,
336 disseminate, make available, transfer, or otherwise communicate
337 orally, in writing, or by electronic or other means, a
338 consumer's personal information by a controller to another
339 controller or a third party for monetary or other valuable
340 consideration.

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

345 1. Allowing a third party to use or advertise or market to
346 a consumer based on a consumer's personal information without
347 disclosure of the personal information to the third party.

348 2. Monetary transactions, nonmonetary transactions, and
349 transactions for other valuable consideration between a
350 controller and a third party for advertising or marketing for

351 the benefit of a controller.

352 (p) "Targeted advertising" means marketing to a consumer
353 or displaying an advertisement to a consumer when the
354 advertisement is selected based on personal information used to
355 predict such consumer's preferences or interests.

356 (q) "Third party" means a person who is not a controller
357 or processor.

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

365 (3) CONSUMER DATA COLLECTION REQUIREMENTS AND
366 RESPONSIBILITIES.—

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

371 1. Any Florida-specific consumer privacy rights.

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

375 3. The consumer's right to request deletion or correction

376 of certain personal information.

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

379 (b) A controller that collects personal information shall,
380 at or before the point of collection, inform, or direct the
381 processor to inform, consumers of the categories of personal
382 information to be collected and the purposes for which the
383 categories of personal information will be used.

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

388 (d) A controller that collects a consumer's personal
389 information shall implement and maintain reasonable security
390 procedures and practices appropriate to the nature of the
391 personal information to protect the personal information from
392 unauthorized or illegal access, destruction, use, modification,
393 or disclosure. A controller must require any processors and
394 third parties to implement and maintain the same or similar
395 security procedures and practices for personal information.

396 (e) A controller shall adopt and implement a retention
397 schedule that prohibits the use or retention of personal
398 information not subject to an exemption by the controller or
399 processor after the satisfaction of the initial purpose for
400 which such information was collected or obtained, after the

401 expiration or termination of the contract pursuant to which the
 402 information was collected or obtained, or 3 years after the
 403 consumer's last interaction with the controller. This paragraph
 404 does not apply to personal information used or retained for the
 405 following purposes:

406 1. Detection of security threats or incidents; protection
 407 against malicious, deceptive, fraudulent, unauthorized, or
 408 illegal activity or access; or prosecution of those responsible
 409 for such activity or access.

410 2. Compliance with a legal obligation, including any
 411 federal retention laws.

412 3. As reasonably needed for the protection of the
 413 controller's interests related to existing disputes, legal
 414 action, or governmental investigations.

415 4. Assuring the physical security of persons or property.

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

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

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

423 2. The sources from which the consumer's personal
 424 information was collected.

425 3. The specific pieces of personal information about the

426 consumer that were sold or shared.

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

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

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

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

439 (d) The controller shall deliver the information required
440 or act on the request in this subsection to a consumer free of
441 charge within 45 days after receiving a verifiable consumer
442 request. The response period may be extended once by 45
443 additional days when reasonably necessary, provided the
444 controller informs the consumer of any such extension within the
445 initial 45-day response period and the reason for the extension.
446 The information must be delivered in a readily usable format. A
447 controller is not obligated to provide information to the
448 consumer if the consumer or a person authorized to act on the
449 consumer's behalf does not provide verification of identity or
450 verification of authorization to act with the permission of the

451 consumer.

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

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

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

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

462 (b) A controller that receives a verifiable consumer
463 request to delete the consumer's personal information shall
464 delete the consumer's personal information from its records and
465 direct any processors to delete such information within 90 days
466 of receipt of the verifiable consumer request.

467 (c) A controller or a processor acting pursuant to its
468 contract with the controller may not be required to comply with
469 a consumer's request to delete the consumer's personal
470 information if it is reasonably necessary for the controller or
471 processor to maintain the consumer's personal information to do
472 any of the following:

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

475 2. Fulfill the terms of a written warranty or product

476 recall conducted in accordance with federal law.

477 3. Provide a good or service requested by the consumer, or
478 reasonably anticipated to be requested within the context of a
479 controller's ongoing business relationship with the consumer, or
480 otherwise perform a contract between the controller and the
481 consumer.

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

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

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

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

497 8. Comply with a legal obligation, including any state or
498 federal retention laws.

499 9. Reasonably protect the controller's interests against
500 existing disputes, legal action, or governmental investigations.

501 10. Internally use the consumer's personal information in
 502 a lawful manner.

503 (d) A consumer has the right to make a request to correct
 504 inaccurate personal information to a controller that maintains
 505 inaccurate personal information about the consumer. A controller
 506 that receives a verifiable consumer request to correct
 507 inaccurate personal information shall use commercially
 508 reasonable efforts to correct the inaccurate personal
 509 information as directed by the consumer and direct any
 510 processors to correct such information within 90 days after
 511 receipt of the verifiable consumer request. If a controller
 512 maintains a self-service mechanism to allow a consumer to
 513 correct certain personal information, the controller may require
 514 the consumer to correct their own personal information through
 515 such mechanism.

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

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

522 (b) Notwithstanding paragraph (a), a controller may not
 523 sell or share the personal information of a minor consumer if
 524 the controller has actual knowledge that the consumer is not 16
 525 years of age or older. However, if a consumer who is between 13

HB9

2022

526 and 16 years of age, or if the parent or guardian of a consumer
527 who is 12 years of age or younger, has affirmatively authorized
528 the sale or sharing of such consumer's personal information,
529 then a controller may sell or share such information in
530 accordance with this section. A controller that willfully
531 disregards the consumer's age is deemed to have actual knowledge
532 of the consumer's age. A controller that complies with the
533 verifiable parental consent requirements of the Children's
534 Online Privacy Protection Act, 15 U.S.C. s. 6501 et seq., shall
535 be deemed compliant with any obligation to obtain parental
536 consent.

537 (c) A controller that has received direction prohibiting
538 the sale or sharing of the consumer's personal information is
539 prohibited from selling or sharing the consumer's personal
540 information beginning 48 hours after receipt of such direction,
541 unless the consumer subsequently provides express authorization
542 for the sale or sharing of the consumer's personal information.

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

545 (a) A controller shall:

546 1. In a form that is reasonably accessible to consumers,
547 provide a clear and conspicuous link on the controller's
548 Internet homepage, entitled "Do Not Sell or Share My Personal
549 Information," to an Internet webpage that enables a consumer, or
550 a person authorized by the consumer, to opt-out of the sale or

HB9

2022

551 sharing of the consumer's personal information. A controller may
552 not require a consumer to create an account in order to direct
553 the controller not to sell the consumer's personal information.
554 A controller may accept a request to opt-out received through a
555 user-enabled global privacy control, such as a browser plug-in
556 or privacy setting, device setting, or other mechanism, which
557 communicates or signals the consumer's choice to opt out.

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

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

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

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

573 (a) A controller may charge a consumer who exercised any
574 of the consumer's rights under this section a different price or
575 rate, or provide a different level or quality of goods or

HB9

2022

576 services to the consumer, only if that difference is reasonably
577 related to the value provided to the controller by the
578 consumer's data or is related to a consumer's voluntary
579 participation in a financial incentive program, including a bona
580 fide loyalty, rewards, premium features, discounts, or club card
581 program offered by the controller.

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

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

590 (9) CONTRACTS AND ROLES.—

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

593 1. Prohibit the processor from selling, sharing,
594 retaining, using, or disclosing the personal information other
595 than for the purposes specified in the contract or agreement
596 with the controller;

597 2. Govern the processor's personal information processing
598 procedures with respect to processing performed on behalf of the
599 controller, including processing instructions, the nature and
600 purpose of processing, the type of information subject to

601 processing, the duration of processing, and the rights and
602 obligations of both the controller and processor;

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

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

610 (b) Determining whether a person is acting as a controller
611 or processor with respect to a specific processing of data is a
612 fact-based determination that depends upon the context in which
613 personal information is to be processed. The contract between a
614 controller and processor must reflect their respective roles and
615 relationships related to handling personal information. A
616 processor that continues to adhere to a controller's
617 instructions with respect to a specific processing of personal
618 information remains a processor.

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

624 (d) A processor or third party must require any
625 subcontractor to meet the same obligations of such processor or

626 third party with respect to personal information.

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

631 (f) Any provision of a contract or agreement of any kind
632 that waives or limits in any way a consumer's rights under this
633 section, including, but not limited to, any right to a remedy or
634 means of enforcement, is deemed contrary to public policy and is
635 void and unenforceable. This section does not prevent a consumer
636 from declining to request information from a controller,
637 declining to opt-out of a controller's sale or sharing of the
638 consumer's personal information, or authorizing a controller to
639 sell or share the consumer's personal information after
640 previously opting out.

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

642 (a) A Florida consumer may only bring a civil action
643 against a controller, processor, or person pursuant to this
644 section for the following:

645 1. Failure to delete or correct a consumer's personal
646 information pursuant to this section after receiving a
647 verifiable consumer request or directions to delete or correct
648 from a controller unless the controller, processor, or person
649 qualifies for an exception to the requirements to delete or
650 correct under this section.

HB9

2022

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

654 3. Selling or sharing the personal information of a
655 consumer age 16 or younger without obtaining consent as required
656 by this section.

657 (b) A court may grant the following relief to a consumer:

658 1. Damages in an amount not less than \$100 and not greater
659 than \$750 per consumer per incident or actual damages, whichever
660 is greater.

661 2. Injunctive or declaratory relief.

662 (c) Upon prevailing, the consumer shall recover reasonable
663 attorney fees and costs.

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

666 (e) Liability for a tort, contract claim, or consumer
667 protection claim which is unrelated to an action brought under
668 subsection (10) or subsection (11) does not arise solely from
669 the failure of a controller, processor, or person to comply with
670 this section and evidence of such may only be used as the basis
671 to prove a cause of action under this subsection.

672 (11) ENFORCEMENT AND IMPLEMENTATION BY THE DEPARTMENT.—

673 (a) Any violation of this section is an unfair and
674 deceptive trade practice actionable under part II of chapter 501
675 solely by the department against a controller, processor, or

676 person. If the department has reason to believe that any
677 controller, processor, or person is in violation of this
678 section, the department, as the enforcement authority, may bring
679 an action against such controller, processor, or person for an
680 unfair or deceptive act or practice. For the purpose of bringing
681 an action pursuant to this section, ss. 501.211 and 501.212 do
682 not apply. Civil penalties may be tripled if the violation:
683 1. Involves a consumer who the controller, processor, or
684 person has actual knowledge is 16 years of age or younger; or
685 2. Is based on paragraph (10) (a).
686 (b) After the department has notified a controller,
687 processor, or person in writing of an alleged violation, the
688 department may in its discretion grant a 45-day period to cure
689 the alleged violation. The 45-day cure period does not apply to
690 a violation of subparagraph (10) (a)1. The department may
691 consider the number and frequency of violations, the substantial
692 likelihood of injury to the public, and the safety of persons or
693 property when determining whether to grant 45 days to cure and
694 the issuance of a letter of guidance. If the violation is cured
695 to the satisfaction of the department and proof of such cure is
696 provided to the department, the department in its discretion may
697 issue a letter of guidance. If the controller, processor, or
698 person fails to cure the violation within 45 days, the
699 department may bring an action against the controller,
700 processor, or person for the alleged violation.

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

703 (d) By February 1 of each year, the department shall
704 submit a report to the President of the Senate and the Speaker
705 of the House of Representatives describing any actions taken by
706 the department to enforce this section. The report shall include
707 statistics and relevant information detailing:

708 1. The number of complaints received;

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

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

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

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

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

726 business in this state, and is therefore subject to the
 727 jurisdiction of the courts of this state.

728 (13) PREEMPTION.—This section is a matter of statewide
 729 concern and supersedes all rules, regulations, codes,
 730 ordinances, and other laws adopted by a city, county, city and
 731 county, municipality, or local agency regarding the collection,
 732 processing, sharing, or sale of consumer personal information by
 733 a controller or processor. The regulation of the collection,
 734 processing, sharing, or sale of consumer personal information by
 735 a controller or processor is preempted to the state.

736 Section 2. Paragraph (g) of subsection (1) of section
 737 501.171, Florida Statutes, is amended to read:

738 501.171 Security of confidential personal information.—

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

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

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

745 (I) A social security number;

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

750 (III) A financial account number or credit or debit card

HB9

2022

751 number, in combination with any required security code, access
752 code, or password that is necessary to permit access to an
753 individual's financial account;

754 (IV) Any information regarding an individual's medical
755 history, mental or physical condition, or medical treatment or
756 diagnosis by a health care professional; or

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

760 (VI) An individual's biometric information as defined in
761 s. 501.173(2).

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

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

772 Section 3. This act shall take effect July 1, 2023.