



181372

LEGISLATIVE ACTION

Senate	.	House
Comm: RCS	.	
04/24/2023	.	
	.	
	.	
	.	

---

The Committee on Rules (Bradley) recommended the following:

**Senate Amendment (with title amendment)**

Delete everything after the enacting clause  
and insert:

Section 1. Section 112.23, Florida Statutes, is created to  
read:

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

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

(a) "Governmental entity" means any state, county,  
district, authority, or municipal officer, department, division,



12 board, bureau, commission, or other separate unit of government  
13 created or established by law, including, but not limited to,  
14 the Commission on Ethics, the Public Service Commission, the  
15 Office of Public Counsel, and any other public or private  
16 agency, person, partnership, corporation, or business entity  
17 acting on behalf of any public agency.

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

21 (2) An officer or a salaried employee of a governmental  
22 entity may not use his or her position or any state resources to  
23 communicate with a social media platform to request the social  
24 media platform to remove content or accounts from the social  
25 media platform.

26 (3) A governmental entity, or an officer or a salaried  
27 employee acting on behalf of a governmental entity, may not  
28 initiate or maintain any agreements or working relationships  
29 with a social media platform for the purpose of content  
30 moderation.

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

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

40 (b) An attempt to remove content that pertains to the



41 commission of a crime or violation of this state's public  
42 records law.

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

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

48 Section 2. The Division of Law Revision is directed to:

49 (1) Redesignate current parts V, VI, and VII of chapter  
50 501, Florida Statutes, as parts VI, VII, and VIII of chapter  
51 501, Florida Statutes, respectively; and

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

55 Section 3. Section 501.701, Florida Statutes, is created to  
56 read:

57 501.701 Short title.—This part may be cited as the "Florida  
58 Digital Bill of Rights."

59 Section 4. Section 501.702, Florida Statutes, is created to  
60 read:

61 501.702 Definitions.—As used in this part, the term:

62 (1) "Affiliate" means a legal entity that controls, is  
63 controlled by, or is under common control with another legal  
64 entity or that shares common branding with another legal entity.

65 For purposes of this subsection, the term "control" or  
66 "controlled" means any of the following:

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



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

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

75 (2) "Aggregate consumer information" means information that  
76 relates to a group or category of consumers, from which the  
77 identity of an individual consumer has been removed and is not  
78 reasonably capable of being directly or indirectly associated or  
79 linked with any consumer, household, or device. The term does  
80 not include information about a group or category of consumers  
81 used to facilitate targeted advertising or the display of ads  
82 online. The term does not include personal information that has  
83 been deidentified.

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

90 (4) "Biometric data" means data generated by automatic  
91 measurements of an individual's biological characteristics. The  
92 term includes fingerprints, voiceprints, eye retinas or irises,  
93 or other unique biological patterns or characteristics used to  
94 identify a specific individual. The term does not include  
95 physical or digital photographs, video or audio recordings or  
96 data generated from video or audio recordings, or information  
97 collected, used, or stored for health care treatment, payment,  
98 or operations under the Health Insurance Portability and



181372

99 Accountability Act of 1996, 42 U.S.C. ss. 1320d et seq.

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

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

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

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

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

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

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

122 (9) "Controller" means

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

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



181372

- 128       2. Conducts business in this state;
- 129       3. Collects personal data about consumers, or is the entity  
130 on behalf of which such information is collected;
- 131       4. Determines the purposes and means of processing personal  
132 data about consumers alone or jointly with others;
- 133       5. Makes in excess of \$1 billion in global gross annual  
134 revenues; and
- 135       6. Satisfies at least one of the following:
- 136       a. Derives 50 percent or more of its global gross annual  
137 revenues from the sale of advertisements, including providing  
138 targeted advertising or the sale of ads online;
- 139       b. Operates a consumer smart speaker and voice command  
140 component service with an integrated virtual assistant connected  
141 to a cloud computing service that uses hands-free verbal  
142 activation. For purposes of this sub-subparagraph, a consumer  
143 smart speaker and voice command component service does not  
144 include a motor vehicle or speaker or device associated with or  
145 connected to a vehicle which is operated by a motor vehicle  
146 manufacturer or a subsidiary or affiliate thereof; or
- 147       c. Operates an app store or a digital distribution platform  
148 that offers at least 250,000 different software applications for  
149 consumers to download and install.
- 150       (b) Any entity that controls or is controlled by a  
151 controller. As used in this paragraph, the term "control" means:
- 152       1. Ownership of, or the power to vote, more than 50 percent  
153 of the outstanding shares of any class of voting security of a  
154 controller;
- 155       2. Control in any manner over the election of a majority of  
156 the directors, or of individuals exercising similar functions;



181372

157 or

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

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

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

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

172 (a) Financial and lending services.

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

174 (c) Education enrollment.

175 (d) Employment opportunities.

176 (e) Criminal justice.

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

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

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

184 (15) "Health record" means any written, printed, or  
185 electronically recorded material maintained by a health care



181372

186 provider in the course of providing health care services to an  
187 individual which concerns the individual and the services  
188 provided. The term includes any of the following:

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

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

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

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

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

201 (a) An organization exempt from federal taxation under s.  
202 501(a) of the Internal Revenue Code of 1986 by virtue of being  
203 listed as an exempt organization under s. 501(c) (3), s.  
204 501(c) (4), s. 501(c) (6), or s. 501(c) (12) of that code.

205 (b) A political organization.

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

214 (20) "Political organization" means a party, a committee,





181372

215 an association, a fund, or any other organization, regardless of  
216 whether incorporated, organized and operated primarily for the  
217 purpose of influencing or attempting to influence any of the  
218 following:

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

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

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

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

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

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



181372

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

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

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

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

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

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

272       (b) The disclosure of personal data to a third party for



181372

273 purposes of providing a product or service requested by the  
274 consumer.

275 (c) The disclosure of information that the consumer:

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

278 2. Did not restrict to a specific audience.

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

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

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

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

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

299 (c) Personal data collected from a known child.

300 (d) Precise geolocation data.

301 (32) "State agency" means any department, commission,



181372

302 board, office, council, authority, or other agency in the  
303 executive branch of state government created by the State  
304 Constitution or state law. The term includes a postsecondary  
305 education institution.

306 (33) "Targeted advertising" means displaying to a consumer  
307 an advertisement selected based on personal data obtained from  
308 that consumer's activities over time and across nonaffiliated  
309 websites or online applications to predict the consumer's  
310 preferences or interests. The term does not include any of the  
311 following:

312 (a) An advertisement that is:

313 1. Based on activities within a controller's own website or  
314 online application;

315 2. Based on the context of a consumer's current search  
316 query, visit to a website, or use of an online application; or

317 3. Directed to a consumer in response to the consumer's  
318 request for information or feedback.

319 (b) The processing of personal data solely for measuring or  
320 reporting advertising performance, reach, or frequency.

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

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

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

329 Section 5. Section 501.703, Florida Statutes, is created to  
330 read:



181372

331           501.703 Applicability.-  
332           (1) This part applies only to a person who:  
333           (a) Conducts business in this state or produces a product  
334 or service used by residents of this state; and  
335           (b) Processes or engages in the sale of personal data.  
336           (2) This part does not apply to any of the following:  
337           (a) A state agency or a political subdivision of the state.  
338           (b) A financial institution or data subject to Title V,  
339 Gramm-Leach-Bliley Act, 15 U.S.C. ss. 6801 et seq.  
340           (c) A covered entity or business associate governed by the  
341 privacy, security, and breach notification regulations issued by  
342 the United States Department of Health and Human Services, 45  
343 C.F.R. parts 160 and 164, established under the Health Insurance  
344 Portability and Accountability Act of 1996, 42 U.S.C. ss. 1320d  
345 et seq., and the Health Information Technology for Economic and  
346 Clinical Health Act, Division A, Title XIII and Division B,  
347 Title IV, Pub. L. No. 111-5.  
348           (d) A nonprofit organization.  
349           (e) A postsecondary education institution.  
350           (3) This part does not apply to the processing of personal  
351 data by a person in the course of a purely personal or household  
352 activity.  
353           (4) A controller or processor that complies with the  
354 authenticated parental consent requirements of the Children's  
355 Online Privacy Protection Act, 15 U.S.C. ss. 6501 et seq., with  
356 respect to data collected online, is considered to be in  
357 compliance with any requirement to obtain parental consent under  
358 this part.  
359           Section 6. Section 501.704, Florida Statutes, is created to



181372

360 read:

361 501.704 Exemptions.—All of the following information is  
362 exempt from this part:

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

366 (2) Health records.

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

369 (4) Identifiable private information:

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

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

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

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

383 (6) Patient safety work product for purposes of the Patient  
384 Safety and Quality Improvement Act of 2005, 42 U.S.C. ss. 299b-  
385 21 et seq.

386 (7) Information derived from any of the health care-related  
387 information listed in this section which is deidentified in  
388 accordance with the requirements for deidentification under the



181372

389 Health Insurance Portability and Accountability Act of 1996, 42  
390 U.S.C. ss. 1320d et seq.

391 (8) Information originating from, and intermingled to be  
392 indistinguishable with, or information treated in the same  
393 manner as, information exempt under this section which is  
394 maintained by a covered entity or business associate as defined  
395 by the Health Insurance Portability and Accountability Act of  
396 1996, 42 U.S.C. ss. 1320d et seq. or by a program or a qualified  
397 service organization as defined by 42 U.S.C. s. 290dd-2.

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

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

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

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

417 (13) Personal data collected, processed, sold, or disclosed



181372

418 in compliance with the Driver's Privacy Protection Act of 1994,  
419 18 U.S.C. ss. 2721 et seq.

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

422 (15) Personal data collected, processed, sold, or disclosed  
423 in compliance with the Farm Credit Act of 1971, 12 U.S.C. ss.  
424 2001 et seq.

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

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

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

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

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





181372

447 this act are preempted by 49 U.S.C. s. 41713.

448 (21) Personal data shared between a manufacturer of a  
449 tangible product and authorized third-party distributors or  
450 vendors of the product, as long as such personal data is used  
451 solely for advertising, marketing, or servicing the product that  
452 is acquired directly through such manufacturer and such  
453 authorized third-party distributors or vendors. Such personal  
454 data may not be sold or shared unless otherwise authorized under  
455 this part.

456 Section 7. Section 501.705, Florida Statutes, is created to  
457 read:

458 501.705 Consumer rights.—

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

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

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

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

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

475 (d) To obtain a copy of the consumer's personal data in a



181372

476 portable and, to the extent technically feasible, readily usable  
477 format if the data is available in a digital format.

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

480 1. Targeted advertising;

481 2. The sale of personal data; or

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

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

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

489 Section 8. Section 501.706, Florida Statutes, is created to  
490 read:

491 501.706 Controller response to consumer requests.—

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

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

504 (3) If a controller cannot take action regarding the



181372

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

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

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

533 (6) A controller who has obtained personal data about a



181372

534 consumer from a source other than the consumer is considered in  
535 compliance with a consumer's request to delete that personal  
536 data pursuant to s. 501.705(2)(c), by doing any of the  
537 following:

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

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

546 Section 9. Section 501.707, Florida Statutes, is created to  
547 read:

548 501.707 Appeal.—

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

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

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

561 Section 10. Section 501.708, Florida Statutes, is created  
562 to read:



563           501.708 Waiver or limitation of consumer rights  
564 prohibited.—Any provision of a contract or agreement which  
565 waives or limits in any way a consumer right described by s.  
566 501.705, s. 501.706, or s. 501.707 is contrary to public policy  
567 and is void and unenforceable.

568           Section 11. Section 501.709, Florida Statutes, is created  
569 to read:

570           501.709 Submitting consumer requests.—

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

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

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

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

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

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

591           Section 12. Section 501.71, Florida Statutes, is created to



181372

592 read:

593 501.71 Controller duties.—

594 (1) A controller shall:

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

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

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

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

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

612 (c) Discriminate against a consumer for exercising any of  
613 the consumer rights contained in this part, including by denying  
614 goods or services, charging different prices or rates for goods  
615 or services, or providing a different level of quality of goods  
616 or services to the consumer. A controller may offer financial  
617 incentives, including payments to consumers as compensation, for  
618 processing of personal data if the consumer gives the controller  
619 prior consent that clearly describes the material terms of the  
620 financial incentive program and provided that such incentive



621 practices are not unjust, unreasonable, coercive, or usurious in  
622 nature. The consent may be revoked by the consumer at any time.

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

630 (3) Paragraph (2) (c) may not be construed to require a  
631 controller to provide a product or service that requires the  
632 personal data of a consumer which the controller does not  
633 collect or maintain or to prohibit a controller from offering a  
634 different price, rate, level, quality, or selection of goods or  
635 services to a consumer, including offering goods or services for  
636 no fee, if the consumer has exercised the consumer's right to  
637 opt out under s. 501.705(2) or the offer is related to a  
638 consumer's voluntary participation in a bona fide loyalty,  
639 rewards, premium features, discounts, or club card program.

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



181372

650 deception of or harm to consumers through the manipulation of  
651 search results.

652 Section 13. Section 501.711, Florida Statutes, is created  
653 to read:

654 501.711 Privacy notices.-

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

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

661 (b) The purpose of processing personal data.

662 (c) How consumers may exercise their rights under s.  
663 501.705(2), including the process by which a consumer may appeal  
664 a controller's decision with regard to the consumer's request.

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

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

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

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

677 (3) If a controller engages in the sale of personal data  
678 that is biometric data, the controller must provide the





181372

679 following notice: "NOTICE: This website may sell your biometric  
680 personal data." The notice must be posted in accordance with  
681 subsection (1).

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

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

691 Section 14. Section 501.712, Florida Statutes, is created  
692 to read:

693 501.712 Duties of processor.—

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

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

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



181372

708 processor.

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

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

716 (a) Clear instructions for processing data.

717 (b) The nature and purpose of processing.

718 (c) The type of data subject to processing.

719 (d) The duration of processing.

720 (e) The rights and obligations of both parties.

721 (f) A requirement that the processor:

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

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

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

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

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

736 (3) Notwithstanding subparagraph (2)(f)4., a processor may



181372

737 arrange for a qualified and independent assessor to conduct an  
738 assessment of the processor's policies and technical and  
739 organizational measures in support of the requirements under  
740 this part using an appropriate and accepted control standard or  
741 framework and assessment procedure. The processor shall provide  
742 a report of the assessment to the controller upon request.

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

747 (5) A determination as to whether a person is acting as a  
748 controller or processor with respect to a specific processing of  
749 data is a fact-based determination that depends on the context  
750 in which personal data is to be processed. A processor that  
751 continues to adhere to a controller's instructions with respect  
752 to a specific processing of personal data remains in the role of  
753 a processor.

754 Section 15. Section 501.713, Florida Statutes, is created  
755 to read:

756 501.713 Data protection assessments.—

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

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

762 (b) The sale of personal data.

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



181372

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

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

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

773        4. Other substantial injury to consumers.

774        (d) The processing of sensitive data.

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

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

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

785        (b) Factor into the assessment:

786        1. The use of deidentified data;

787        2. The reasonable expectations of consumers;

788        3. The context of the processing; and

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

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



795 assessment and any information contained in the assessment.

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

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

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

805 Section 16. Section 501.714, Florida Statutes, is created  
806 to read:

807 501.714 Deidentified data, pseudonymous data, and aggregate  
808 consumer information.-

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

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

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

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

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

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



824       (a) Reidentify deidentified data or pseudonymous data.  
825       (b) Maintain data in an identifiable form or obtain,  
826 retain, or access any data or technology for the purpose of  
827 allowing the controller or processor to associate a consumer  
828 request with personal data.  
829       (c) Comply with an authenticated consumer rights request  
830 under s. 501.705 if the controller:  
831       1. Is not reasonably capable of associating the request  
832 with the personal data or it would be unreasonably burdensome  
833 for the controller to associate the request with the personal  
834 data;  
835       2. Does not use the personal data to recognize or respond  
836 to the specific consumer who is the subject of the personal data  
837 or associate the personal data with other personal data about  
838 the same specific consumer; and  
839       3. Does not sell the personal data to a third party or  
840 otherwise voluntarily disclose the personal data to a third  
841 party other than a processor, except as otherwise authorized by  
842 this section.  
843       (3) The consumer rights enumerated under s. 501.705(2), and  
844 controller duties imposed under s. 501.71, do not apply to  
845 pseudonymous data or aggregate consumer information in cases in  
846 which the controller is able to demonstrate that any information  
847 necessary to identify the consumer is kept separate and is  
848 subject to effective technical and organizational controls that  
849 prevent the controller from accessing the information.  
850       (4) A controller that discloses pseudonymous data,  
851 deidentified data, or aggregate consumer information shall  
852 exercise reasonable oversight to monitor compliance with any



853 contractual commitments to which the data or information is  
854 subject and shall take appropriate steps to address any breach  
855 of the contractual commitments.

856 Section 17. Section 501.715, Florida Statutes, is created  
857 to read:

858 501.715 Requirements for sensitive data.—

859 (1) A person who meets the requirements of s.  
860 501.702(9)(a)1, (a)2., and (a)3. for the definition of a  
861 controller may not engage in the sale of personal data that is  
862 sensitive data without receiving prior consent from the consumer  
863 or, if the sensitive data is of a known child, without  
864 processing that data with the affirmative authorization for such  
865 processing by a known child who is between 13 and 18 years of  
866 age or in accordance with the Children's Online Privacy  
867 Protection Act, 15 U.S.C. ss. 6501 et seq. for a known child  
868 under the age of 13.

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

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

875 Section 18. Section 501.716, Florida Statutes, is created  
876 to read:

877 501.716 Exemptions for certain uses of consumer personal  
878 data.—

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

881 (a) Comply with federal or state laws, rules, or



882 regulations.

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

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

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

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

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

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

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

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





181372

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

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

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

918 (j) Disclose personal data disclosed when a consumer uses  
919 or directs the controller to intentionally disclose information  
920 to a third party or uses the controller to intentionally  
921 interact with a third party. An intentional interaction occurs  
922 when the consumer intends to interact with the third party, by  
923 one or more deliberate interactions. Hovering over, muting,  
924 pausing, or closing a given piece of content does not constitute  
925 a consumer's intent to interact with a third party.

926 (k) Transfer personal data to a third party as an asset  
927 that is part of a merger, an acquisition, a bankruptcy, or other  
928 transaction in which the third party assumes control of all or  
929 part of the controller, provided that the information is used or  
930 shared in a manner consistent with this part. If a third party  
931 materially alters how it uses or shares the personal data of a  
932 consumer in a manner that is materially inconsistent with the  
933 commitments or promises made at the time of collection, it must  
934 provide prior notice of the new or changed practice to the  
935 consumer. The notice must be sufficiently prominent and robust  
936 to ensure that consumers can easily exercise choices consistent  
937 with this part.

938 (2) This part may not be construed to prevent a controller  
939 or processor from providing personal data concerning a consumer



181372

940 to a person covered by an evidentiary privilege under the laws  
941 of this state as part of a privileged communication.

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

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

949 Section 19. Section 501.717, Florida Statutes, is created  
950 to read:

951 501.717 Collection, use, or retention of data for certain  
952 purposes.—

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

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

959 (b) Effect a product recall.

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

962 (d) Perform internal operations that are:

963 1. Reasonably aligned with the expectations of the  
964 consumer;

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

967 3. Otherwise compatible with processing data in furtherance  
968 of the provision of a product or service specifically requested



181372

969 by a consumer or the performance of a contract to which the  
970 consumer is a party.

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

975 Section 20. Section 501.718, Florida Statutes, is created  
976 to read:

977 501.718 Disclosure of personal data to third-party  
978 controller or processor.—

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

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

993 Section 21. Section 501.719, Florida Statutes, is created  
994 to read:

995 501.719 Processing of certain personal data by controller  
996 or other person.—

997 (1) Personal data processed by a controller pursuant to ss.



998 501.716, 501.717, and 501.718 may not be processed for any  
999 purpose other than those specified in those sections. Personal  
1000 data processed by a controller pursuant to ss. 501.716, 501.717,  
1001 and 501.718 may be processed to the extent that the processing  
1002 of the data is:

1003 (a) Reasonably necessary and proportionate to the purposes  
1004 specified in ss. 501.716, 501.717, and 501.718; and

1005 (b) Adequate, relevant, and limited to what is necessary in  
1006 relation to the purposes specified in ss. 501.716, 501.717, and  
1007 501.718.

1008 (c) Done to assist another controller, processor, or third  
1009 party with any of the purposes specified in s. 501.716, s.  
1010 501.717, or s. 501.718.

1011 (2) A controller or processor that collects, uses, or  
1012 retains personal data for the purposes specified in s.  
1013 501.717(1) must take into account the nature and purpose of such  
1014 collection, use, or retention. Such personal data is subject to  
1015 reasonable administrative, technical, and physical measures to  
1016 protect its confidentiality, integrity, and accessibility and to  
1017 reduce reasonably foreseeable risks of harm to consumers  
1018 relating to the collection, use, or retention of personal data.

1019 (3) A controller or processor shall adopt and implement a  
1020 retention schedule that prohibits the use or retention of  
1021 personal data not subject to an exemption by the controller or  
1022 processor after the satisfaction of the initial purpose for  
1023 which such information was collected or obtained, after the  
1024 expiration or termination of the contract pursuant to which the  
1025 information was collected or obtained, or 2 years after the  
1026 consumer's last interaction with the controller or processor.



1027 This subsection does not apply to personal data reasonably used  
1028 or retained to do any of the following:

1029 (a) Provide a good or service requested by the consumer, or  
1030 reasonably anticipate the request of such good or service within  
1031 the context of a controller's ongoing business relationship with  
1032 the consumer.

1033 (b) Debug to identify and repair errors that impair  
1034 existing intended functionality.

1035 (c) Enable solely internal uses that are reasonably aligned  
1036 with the expectations of the consumer based on the consumer's  
1037 relationship with the controller or that are compatible with the  
1038 context in which the consumer provided the information.

1039 (4) A controller or processor that processes personal data  
1040 pursuant to ss. 501.716, 501.717, and 501.718 bears the burden  
1041 of demonstrating that the processing of the personal data  
1042 qualifies for the exemption and complies with the requirements  
1043 of this section.

1044 Section 22. Section 501.72, Florida Statutes, is created to  
1045 read:

1046 501.72 Enforcement and implementation by the Department of  
1047 Legal Affairs.—

1048 (1) A violation of this part is an unfair and deceptive  
1049 trade practice actionable under part II of this chapter solely  
1050 by the Department of Legal Affairs. If the department has reason  
1051 to believe that a person is in violation of this section, the  
1052 department may, as the enforcing authority, bring an action  
1053 against such person for an unfair or deceptive act or practice.  
1054 For the purpose of bringing an action pursuant to this section,  
1055 ss. 501.211 and 501.212 do not apply. In addition to other



181372

1056 remedies under part II of this chapter, the department may  
1057 collect a civil penalty of up to \$50,000 per violation. Civil  
1058 penalties may be tripled for any of the following violations:  
1059 (a) A violation involving a Florida consumer who is a known  
1060 child. A controller that willfully disregards the consumer's age  
1061 is deemed to have actual knowledge of the consumer's age.  
1062 (b) Failure to delete or correct the consumer's personal  
1063 data pursuant to this section after receiving an authenticated  
1064 consumer request or directions from a controller to delete or  
1065 correct such personal data, unless an exception to the  
1066 requirements to delete or correct such personal data under this  
1067 section applies.  
1068 (c) Continuing to sell or share the consumer's personal  
1069 data after the consumer chooses to opt out under this part.  
1070 (2) After the department has notified a person in writing  
1071 of an alleged violation, the department may grant a 45-day  
1072 period to cure the alleged violation and issue a letter of  
1073 guidance. The 45-day cure period does not apply to an alleged  
1074 violation of paragraph (1)(a). The department may consider the  
1075 number and frequency of violations, the substantial likelihood  
1076 of injury to the public, and the safety of persons or property  
1077 in determining whether to grant 45 calendar days to cure and the  
1078 issuance of a letter of guidance. If the alleged violation is  
1079 cured to the satisfaction of the department and proof of such  
1080 cure is provided to the department, the department may not bring  
1081 an action for the alleged violation but in its discretion may  
1082 issue a letter of guidance that indicates that the person will  
1083 not be offered a 45-day cure period for any future violations.  
1084 If the person fails to cure the alleged violation within 45



181372

1085 calendar days, the department may bring an action against such  
1086 person for the alleged violation.

1087 (3) Any action brought by the department may be brought  
1088 only on behalf of a Florida consumer.

1089 (4) By February 1 of each year, the department shall make a  
1090 report publicly available on the department's website describing  
1091 any actions taken by the department to enforce this section. The  
1092 report must include statistics and relevant information  
1093 detailing all of the following:

1094 (a) The number of complaints received and the categories or  
1095 types of violations alleged by the complainant.

1096 (b) The number and type of enforcement actions taken and  
1097 the outcomes of such actions, including the amount of penalties  
1098 issued and collected.

1099 (c) The number of complaints resolved without the need for  
1100 litigation.

1101 (d) For the report due February 1, 2024, the status of the  
1102 development and implementation of rules to implement this  
1103 section.

1104 (5) The department shall adopt rules to implement this  
1105 section, including standards for authenticated consumer  
1106 requests, enforcement, data security, and authorized persons who  
1107 may act on a consumer's behalf.

1108 (6) The department may collaborate and cooperate with other  
1109 enforcement authorities of the Federal Government or other state  
1110 governments concerning consumer data privacy issues and consumer  
1111 data privacy investigations if such enforcement authorities have  
1112 restrictions governing confidentiality at least as stringent as  
1113 the restrictions provided in this section.



181372

1114           (7) Liability for a tort, contract claim, or consumer  
1115 protection claim unrelated to an action brought under this  
1116 section does not arise solely from the failure of a person to  
1117 comply with this part.

1118           (8) This part does not establish a private cause of action.

1119           (9) The department may employ or use the legal services of  
1120 outside counsel and the investigative services of outside  
1121 personnel to fulfill the obligations of this section.

1122           (10) For purposes of bringing an action pursuant to this  
1123 section, any person who meets the definition of controller as  
1124 defined in this part who collects, shares, or sells the personal  
1125 data of Florida consumers is considered to be engaged in both  
1126 substantial and not isolated activities within this state and  
1127 operating, conducting, engaging in, or carrying on a business,  
1128 and doing business in this state, and is, therefore, subject to  
1129 the jurisdiction of the courts of this state.

1130           Section 23. Section 501.721, Florida Statutes, is created  
1131 to read:

1132           501.721 Preemption.—This part is a matter of statewide  
1133 concern and supersedes all rules, regulations, codes,  
1134 ordinances, and other laws adopted by a city, county, city and  
1135 county, municipality, or local agency regarding the collection,  
1136 processing, sharing, or sale of consumer personal data by a  
1137 controller or processor. The regulation of the collection,  
1138 processing, sharing, or sale of consumer personal data by a  
1139 controller or processor is preempted to the state.

1140           Section 24. Paragraph (g) of subsection (1) of section  
1141 501.171, Florida Statutes, is amended to read:

1142           501.171 Security of confidential personal information.—





181372

1143 (1) DEFINITIONS.—As used in this section, the term:  
1144 (g)1. “Personal information” means either of the following:  
1145 a. An individual’s first name or first initial and last  
1146 name in combination with any one or more of the following data  
1147 elements for that individual:  
1148 (I) A social security number;  
1149 (II) A driver license or identification card number,  
1150 passport number, military identification number, or other  
1151 similar number issued on a government document used to verify  
1152 identity;  
1153 (III) A financial account number or credit or debit card  
1154 number, in combination with any required security code, access  
1155 code, or password that is necessary to permit access to an  
1156 individual’s financial account;  
1157 (IV) Any information regarding an individual’s medical  
1158 history, mental or physical condition, or medical treatment or  
1159 diagnosis by a health care professional; ~~or~~  
1160 (V) An individual’s health insurance policy number or  
1161 subscriber identification number and any unique identifier used  
1162 by a health insurer to identify the individual;  
1163 (VI) An individual’s biometric data as defined in s.  
1164 501.702; or  
1165 (VII) Any information regarding an individual’s  
1166 geolocation.  
1167 b. A user name or e-mail address, in combination with a  
1168 password or security question and answer that would permit  
1169 access to an online account.  
1170 2. The term does not include information about an  
1171 individual that has been made publicly available by a federal,



181372

1172 state, or local governmental entity. The term also does not  
1173 include information that is encrypted, secured, or modified by  
1174 any other method or technology that removes elements that  
1175 personally identify an individual or that otherwise renders the  
1176 information unusable.

1177 Section 25. Subsection (1) of section 16.53, Florida  
1178 Statutes, is amended, and subsection (8) is added to that  
1179 section, to read:

1180 16.53 Legal Affairs Revolving Trust Fund.—

1181 (1) There is created in the State Treasury the Legal  
1182 Affairs Revolving Trust Fund, from which the Legislature may  
1183 appropriate funds for the purpose of funding investigation,  
1184 prosecution, and enforcement by the Attorney General of the  
1185 provisions of the Racketeer Influenced and Corrupt Organization  
1186 Act, the Florida Deceptive and Unfair Trade Practices Act, the  
1187 Florida False Claims Act, ~~or~~ state or federal antitrust laws, or  
1188 part V of chapter 501.

1189 (8) All moneys recovered by the Attorney General for  
1190 attorney fees, costs, and penalties in an action for a violation  
1191 of part V of chapter 501 must be deposited in the trust fund.

1192 Section 26. This act shall take effect July 1, 2023

1193  
1194 ===== T I T L E A M E N D M E N T =====

1195 And the title is amended as follows:

1196 Delete everything before the enacting clause  
1197 and insert:

1198 A bill to be entitled  
1199 An act relating to technology transparency; creating  
1200 s. 112.23, F.S.; defining terms; prohibiting officers



1201 or salaried employees of governmental entities from  
1202 using their positions or state resources to make  
1203 certain requests of social media platforms;  
1204 prohibiting governmental entities from initiating or  
1205 maintaining agreements or working relationships with  
1206 social media platforms under a specified circumstance;  
1207 providing exceptions; providing directives to the  
1208 Division of Law Revision; creating s. 501.701, F.S.;  
1209 providing a short title; creating s. 501.702, F.S.;  
1210 defining terms; creating s. 501.703, F.S.; providing  
1211 applicability; creating s. 501.704, F.S.; providing  
1212 exemptions; creating s. 501.705, F.S.; providing that  
1213 a consumer may submit requests to controllers to  
1214 exercise specified rights; requiring controllers to  
1215 comply with certain authenticated consumer requests;  
1216 creating s. 501.706, F.S.; providing timeframes within  
1217 which controllers must respond to consumer requests;  
1218 providing notice requirements for controllers that  
1219 cannot take action regarding a consumer's request;  
1220 providing that controllers are not required to comply  
1221 with certain consumer requests; providing notice  
1222 requirements for controllers' compliance with consumer  
1223 requests; requiring responses to consumer requests to  
1224 be made free of charge; providing exceptions;  
1225 specifying the methods by which controllers may be  
1226 considered to be in compliance with consumer requests  
1227 for the controller to delete their personal data;  
1228 creating s. 501.707, F.S.; requiring controllers to  
1229 establish a process for consumers to appeal the



1230 controller's refusal to take action on the consumer's  
1231 request within a specified timeframe; providing  
1232 requirements for such process; creating s. 501.708,  
1233 F.S.; providing that contracts or agreements that  
1234 waive or limit specified consumer rights are void and  
1235 unenforceable; creating s. 501.709, F.S.; requiring  
1236 controllers to establish methods for submitting  
1237 consumer requests; prohibiting controllers from  
1238 requiring consumers to create new accounts to exercise  
1239 their consumer rights; requiring controllers to  
1240 provide a certain mechanism on their websites for  
1241 consumers to submit certain requests; creating s.  
1242 501.71, F.S.; requiring controllers to limit the  
1243 collection of personal data according to certain  
1244 parameters; requiring controllers to establish,  
1245 implement, and maintain specified practices regarding  
1246 personal data; prohibiting controllers from taking  
1247 certain actions regarding a consumer's personal data;  
1248 prohibiting controllers from discriminating against  
1249 consumers exercising their consumer rights; providing  
1250 construction; requiring a controller that operates a  
1251 search engine to make certain information available on  
1252 its webpage; creating s. 501.711, F.S.; requiring  
1253 controllers to provide consumers with privacy notices  
1254 that meet certain requirements; requiring controllers  
1255 that engage in the sale of sensitive or biometric  
1256 personal data to provide notices that meet certain  
1257 requirements; requiring controllers that sell personal  
1258 data or process personal data for targeted advertising



1259 to disclose certain information; prohibiting  
1260 controllers from collecting additional categories of  
1261 personal information or using such information for  
1262 additional purposes without providing specified  
1263 notice; creating s. 501.712, F.S.; requiring  
1264 processors to adhere to controller instructions and to  
1265 assist the controller in meeting or complying with  
1266 certain requirements; providing requirements for  
1267 contracts between controllers and processors regarding  
1268 data processing procedures; providing construction;  
1269 providing that the determination of whether a person  
1270 is acting as a controller or processor is a fact-based  
1271 determination; creating s. 501.713, F.S.; requiring  
1272 controllers to conduct and document data protection  
1273 assessments of specified processing activities  
1274 involving personal data; providing requirements for  
1275 such assessments; providing applicability; creating s.  
1276 501.714, F.S.; requiring controllers in possession of  
1277 deidentified data to take certain actions; providing  
1278 construction; providing that specified consumer rights  
1279 and controller duties do not apply to pseudonymous  
1280 data or aggregate consumer information under certain  
1281 circumstances; requiring controllers that disclose  
1282 pseudonymous data, deidentified data, or aggregate  
1283 consumer information to exercise reasonable oversight  
1284 and take appropriate steps to address breaches of  
1285 contractual agreements; creating s. 501.715, F.S.;  
1286 requiring certain persons to receive consumer consent  
1287 before engaging in the sale of sensitive personal



1288 data; requiring a specified notice; providing for  
1289 penalties; creating s. 501.716, F.S.; providing  
1290 exemptions for specified controller or processor uses  
1291 of consumer personal data; providing that controllers  
1292 or processors may provide personal data concerning a  
1293 consumer to certain covered persons; creating s.  
1294 501.717, F.S.; authorizing controllers and processors  
1295 to collect, use, or retain data for specified  
1296 purposes; providing that certain requirements do not  
1297 apply if such compliance would violate certain laws;  
1298 creating s. 501.718, F.S.; providing circumstances  
1299 under which processors are not in violation of this  
1300 act for the disclosure of personal data to a third-  
1301 party controller or processor; providing that third-  
1302 party controllers or processors that comply with this  
1303 part are not liable for violations committed by  
1304 controllers or processors from whom they receive  
1305 personal data; creating s. 501.719, F.S.; providing  
1306 requirements for the processing of certain personal  
1307 data by controllers; requiring controllers and  
1308 processors to adopt and implement a retention schedule  
1309 that meets certain requirements; requiring controllers  
1310 or processors that process certain personal data to  
1311 demonstrate that such processing qualifies for a  
1312 specified exemption; creating s. 501.72, F.S.;  
1313 authorizing the Department of Legal Affairs to bring  
1314 an action under the Florida Deceptive and Unfair Trade  
1315 Practices Act for violations of the act; providing for  
1316 civil penalties; providing for enhanced civil



1317 penalties for certain violations; authorizing the  
1318 department to grant a specified timeframe within which  
1319 a an alleged violation may be cured; providing an  
1320 exception; providing certain factors the department  
1321 may take into consideration; requiring the department  
1322 to make a report regarding certain enforcement actions  
1323 publicly available on the department's website;  
1324 providing requirements for the report; requiring the  
1325 department to adopt rules; authorizing the department  
1326 to collaborate and cooperate with specified  
1327 enforcement authorities; specifying that the act does  
1328 not create a private cause of action; authorizing the  
1329 department to employ or use outside legal counsel for  
1330 specified purposes; providing for jurisdiction;  
1331 creating s. 501.721, F.S.; declaring that the act is a  
1332 matter of statewide concern; preempting the  
1333 collection, processing, sharing, and sale of consumer  
1334 personal data to the state; amending s. 501.171, F.S.;  
1335 revising the definition of the term "personal  
1336 information"; amending s. 16.53, F.S.; requiring that  
1337 certain attorney fees, costs, and penalties recovered  
1338 by the Attorney General be deposited in the Legal  
1339 Affairs Revolving Trust Fund; providing an effective  
1340 date.