

**HB351 ENROLLED**



1 HB351  
2 XDP66ZZ-3  
3 By Representative Shaw  
4 RFD: Commerce and Small Business  
5 First Read: 29-Jan-26



## HB351 Enrolled

1 Enrolled, An Act,

2

3 Relating to data privacy; to authorize a consumer to  
4 take certain actions regarding the consumer's personal data;  
5 to regulate the manner in which a controller may process  
6 personal data; to provide for the obligations of a data  
7 processor; to regulate the processing of deidentified data;  
8 and to provide for enforcement of this act.

9 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

10 Section 1. This act shall be known as the Alabama  
11 Personal Data Protection Act.

12 Section 2. For the purposes of this act, the following  
13 terms have the following meanings:

14 (1) AFFILIATE. A legal entity that shares common  
15 branding with another legal entity or that controls, is  
16 controlled by, or is under common control with another legal  
17 entity.

18 (2) AUTHENTICATE. To use reasonable methods to  
19 determine that a request to exercise any of the consumer  
20 rights afforded under this act is being made by, or on behalf  
21 of, a consumer who is entitled to exercise those consumer  
22 rights with respect to the consumer's personal data at issue.

23 (3) BIOMETRIC DATA. Data generated by automatic  
24 measurements of an individual's biological characteristics,  
25 such as a fingerprint, voiceprint, retina, or iris, that are  
26 used to identify a specific individual. The term does not  
27 include any of the following:

28 a. A digital or physical photograph.



## HB351 Enrolled

29           b. An audio or video recording.

30           c. Any data generated from paragraph a. or b. unless  
31 the data is used to identify a specific individual.

32           (4) CHILD. An individual under 13 years of age.

33           (5) CONSENT. A clear affirmative act signifying a  
34 consumer's freely given, specific, informed, and unambiguous  
35 agreement to allow the processing of personal data relating to  
36 the consumer, including, but not limited to, a written  
37 statement or a statement by electronic means. The term does  
38 not include any of the following:

39           a. Acceptance of a general or broad term of use or  
40 similar document that contains descriptions of personal data  
41 processing along with other unrelated information.

42           b. Hovering over, muting, or pausing a given piece of  
43 content.

44           c. An agreement obtained using dark patterns.

45           (6) CONSUMER. An individual who is a resident of this  
46 state. The term does not include an individual acting in a  
47 commercial or employment context or as an employee, owner,  
48 director, officer, or contractor of a company, partnership,  
49 sole proprietorship, nonprofit, or government agency whose  
50 communications or transactions with the controller occur  
51 solely within the context of that individual's role with the  
52 company, partnership, sole proprietorship, nonprofit, or  
53 government agency.

54           (7) CONTROL. Any of the following:

55           a. Ownership of or the power to vote more than 50  
56 percent of the outstanding shares of any class of voting



## HB351 Enrolled

57 security of a company.

58           b. Control in any manner over the election of a  
59 majority of the directors or of individuals exercising similar  
60 functions.

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

63           (8) CONTROLLER. An individual or legal entity that,  
64 alone or jointly with others, determines the purposes and  
65 means of processing personal data.

66           (9) DARK PATTERN. A user interface designed or  
67 manipulated with the effect of substantially subverting or  
68 impairing user autonomy, decision-making, or choice.

69           (10) DEIDENTIFIED DATA. Data that cannot be used to  
70 reasonably infer information about or otherwise be linked to  
71 an identified or identifiable individual or a device linked to  
72 an identified or identifiable individual if the controller  
73 that possesses the data does all of the following:

74           a. Takes reasonable measures to ensure that the data  
75 cannot be associated with an individual.

76           b. Publicly commits to process the data in a  
77 deidentified fashion only and to not attempt to reidentify the  
78 data.

79           c. Contractually obligates any recipients of the data  
80 to satisfy the criteria set forth in Section 11(a) and (b).

81           (11) IDENTIFIABLE INDIVIDUAL. An individual who can be  
82 readily identified, directly or indirectly.

83           (12) NONPROFIT ENTITY. As defined in Section  
84 10A-1-1.03, Code of Alabama 1975.



## HB351 Enrolled

85 (13) PERSONAL DATA. Any information that is linked or  
86 reasonably linkable to an identified or identifiable  
87 individual. The term does not include deidentified data or  
88 publicly available information.

89 (14) PRECISE GEOLOCATION DATA. Information derived from  
90 technology, including, but not limited to, global positioning  
91 system level latitude and longitude coordinates, which  
92 directly identifies the specific location of an individual  
93 with precision and accuracy within a radius of 1,750 feet. The  
94 term does not include the content of communications or any  
95 data generated by or connected to advanced utility metering  
96 infrastructure systems or equipment for use by a utility.

97 (15) PROCESS. Any operation or set of operations,  
98 whether by manual or automated means, performed on personal  
99 data or on sets of personal data, including, but not limited  
100 to, the collection, use, storage, disclosure, analysis,  
101 deletion, or modification of personal data.

102 (16) PROCESSOR. An individual or legal entity that  
103 processes personal data on behalf of a controller.

104 (17) PROFILING. Any form of solely-automated processing  
105 performed on personal data to evaluate, analyze, or predict  
106 personal aspects related to an identified or identifiable  
107 individual's economic situation, health, personal preferences,  
108 interests, reliability, behavior, location, or movements.

109 (18) PSEUDONYMOUS DATA. Personal data that cannot be  
110 attributed to a specific individual without the use of  
111 additional information, provided the additional information is  
112 kept separately and is subject to appropriate technical and



## HB351 Enrolled

113 organizational measures to ensure that the personal data is  
114 not attributable to an identified or identifiable individual.

115 (19) PUBLICLY AVAILABLE INFORMATION. Either of the  
116 following:

117 a. Information that is lawfully made available through  
118 federal, state, or local government records or widely  
119 distributed media.

120 b. Information that a controller has a reasonable basis  
121 to believe a consumer has lawfully made available to the  
122 public.

123 (20) SALE OF PERSONAL DATA. The exchange of personal  
124 data for monetary consideration by a controller to a third  
125 party, or for other valuable consideration by a controller to  
126 a third party where the controller receives a material benefit  
127 and the third party is not restricted in its subsequent uses  
128 of the personal data. The term does not include any of the  
129 following:

130 a. The disclosure of personal data to a processor that  
131 processes the personal data on behalf of the controller.

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

135 c. The disclosure or transfer of personal data to an  
136 affiliate of the controller.

137 d. The disclosure of personal data in which the  
138 consumer directs the controller to disclose the personal data  
139 or intentionally uses the controller to interact with a third  
140 party.



## HB351 Enrolled

141 e. The disclosure of personal data that the consumer  
142 intentionally made available to the public via a channel of  
143 mass media and did not restrict to a specific audience.

144 f. The disclosure or transfer of personal data to a  
145 third party as an asset that is part of a merger, acquisition,  
146 bankruptcy, or other transaction, or a proposed merger,  
147 acquisition, bankruptcy, or other transaction in which the  
148 third party assumes control of all or part of the controller's  
149 assets.

150 g. The disclosure or transfer of personal data to a  
151 third party for the purposes of providing analytics services.

152 h. The disclosure or transfer of personal data to a  
153 third party for the purposes of providing marketing services  
154 solely to the controller.

155 (21) SENSITIVE DATA. Personal data that includes any of  
156 the following:

157 a. Data revealing racial or ethnic origin, religious  
158 beliefs, a mental or physical health condition or diagnosis,  
159 information about an individual's sex life, sexual  
160 orientation, or citizenship or immigration status.

161 b. The processing of genetic or biometric data for the  
162 purpose of uniquely identifying an individual.

163 c. Personal data collected from a known child.

164 d. Precise geolocation data.

165 (22) SIGNIFICANT DECISION. A decision made by a  
166 controller that results in the provision or denial by the  
167 controller of credit or lending services, housing, insurance,  
168 education enrollment or opportunity, criminal justice,



## HB351 Enrolled

169 employment opportunity, health care service, or access to  
170 basic necessities such as food or water.

171 (23) TARGETED ADVERTISING. Displaying advertisements to  
172 a consumer in which the advertisement is selected based on  
173 personal data obtained or inferred from that consumer's  
174 activities over time and across nonaffiliated Internet  
175 websites or online applications to predict the consumer's  
176 preferences or interests. The term does not include any of the  
177 following:

178 a. Advertisements based on activities within a  
179 controller's own Internet websites or online applications.

180 b. Advertisements based on the context of a consumer's  
181 current search query or visit to any Internet website or  
182 online application.

183 c. Advertisements directed to a consumer in response to  
184 the consumer's request for information or feedback.

185 d. Processing personal data solely to measure or report  
186 advertising frequency, performance, or reach.

187 (24) THIRD PARTY. An individual or legal entity other  
188 than a consumer, controller, processor, or an affiliate of the  
189 controller or processor.

190 (25) TRADE SECRET. As defined in Section 8-27-2, Code  
191 of Alabama 1975.

192 Section 3. The provisions of this act apply to persons  
193 that conduct business in this state or persons that produce  
194 products or services that are targeted to residents of this  
195 state and that meet either of the following qualifications:

196 (1) Control or process the personal data of more than



## HB351 Enrolled

197 25,000 consumers, excluding personal data controlled or  
198 processed solely for the purpose of completing a payment  
199 transaction.

200 (2) Derive more than 25 percent of gross revenue from  
201 the sale of personal data, regardless of the number of  
202 consumers whose data the person controls or processes.

203 Section 4. (a) Notwithstanding any other provisions of  
204 this act, this act shall not apply to any of the following:

205 (1)a. A political subdivision of the state.

206 b. Any board, authority, district, or public  
207 corporation organized pursuant to Title 11, Code of Alabama  
208 1975, or Chapter 7 of Title 39, Code of Alabama 1975.

209 (2) A two-year or four-year institution of higher  
210 education, including affiliates of a two-year or four-year  
211 institution of higher education.

212 (3) A national securities association that is  
213 registered under 15 U.S.C. § 78o-3.

214 (4) A financial institution or an affiliate of a  
215 financial institution governed by 15 U.S.C. Chapter 94.

216 (5) A financial institution or an affiliate of a  
217 financial institution governed by, or personal data collected,  
218 processed, sold, or disclosed in accordance with Title V of  
219 the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et. seq.

220 (6) A covered entity or business associate as defined  
221 in the privacy regulations of 45 C.F.R. § 160.103.

222 (7) A business, including an organization cooperatively  
223 organized under Chapter 6 of Title 37, Code of Alabama 1975,  
224 or an entity that is an instrumentality of a municipal



## HB351 Enrolled

225 corporation, with fewer than 500 employees, provided the  
226 business does not engage in the sale of personal data.

227 (8) A nonprofit entity, as defined in Section  
228 10A-1-1.03, Code of Alabama 1975, with less than 100  
229 employees, provided the entity does not engage in the sale of  
230 personal data.

231 (9) Any person or entity regulated by Chapter 6 of  
232 Title 8, Code of Alabama 1975.

233 (10) Any person or entity regulated by Chapter 7A of  
234 Title 8, Code of Alabama 1975.

235 (11) Any trade association explicitly authorized to  
236 receive documents or evidence pursuant to Section 27-12A-23,  
237 Code of Alabama 1975.

238 (12)a. A political action committee, political party,  
239 or principal campaign committee, as defined in Section 17-5-2,  
240 Code of Alabama 1975, or any political organization as defined  
241 in 26 U.S.C. §527.

242 b. A business entity that sells data primarily to a  
243 political action committee, political party, or principal  
244 campaign committee, as defined in Section 17-5-2, Code of  
245 Alabama 1975, or any political organization as defined in 26  
246 U.S.C. §527.

247 (13) An electric provider as defined under Chapter 16  
248 of Title 37, Code of Alabama 1975, that is subject to the  
249 requirements or reliability standards of the North American  
250 Electric Reliability Corporation.

251 (b) This act shall not apply to any of the following  
252 information or data:



## HB351 Enrolled

253 (1) Protected health information under the privacy  
254 regulations of the federal Health Insurance Portability and  
255 Accountability Act of 1996 and related regulations.

256 (2) Patient-identifying information for the purposes of  
257 42 C.F.R. Part 2, established pursuant to 42 U.S.C. § 290dd-2.

258 (3) Identifiable private information for the purposes  
259 of 45 C.F.R. Part 46.

260 (4) Identifiable private information that is otherwise  
261 collected as part of human subjects research pursuant to the  
262 good clinical practice guidelines issued by the International  
263 Council for Harmonisation of Technical Requirements for  
264 Pharmaceuticals for Human Use.

265 (5) The protection of human subjects under 21 C.F.R.  
266 Parts 50 and 56, or personal data used or shared in research  
267 as defined in the federal Health Insurance Portability and  
268 Accountability Act of 1996 and 45 C.F.R. § 164.501, that is  
269 conducted in accordance with applicable law.

270 (6) Information or documents created for the purposes  
271 of the federal Health Care Quality Improvement Act of 1986.

272 (7) Patient safety work products for the purposes of  
273 the federal Patient Safety and Quality Improvement Act of  
274 2005.

275 (8) Information derived from any of the health care  
276 related information listed in this subsection which is  
277 deidentified in accordance with the requirements for  
278 deidentification pursuant to the privacy regulations of the  
279 federal Health Insurance Portability and Accountability Act of  
280 1996.



## HB351 Enrolled

281 (9) Information derived from any of the health care  
282 related information listed in this subsection which is  
283 included in a limited data set as described in 45 C.F.R. §  
284 164.514(e), to the extent that the information is used,  
285 disclosed, and maintained in a manner specified in 45 C.F.R. §  
286 164.514(e).

287 (10) Information originating from and intermingled to  
288 be indistinguishable with or information treated in the same  
289 manner as information exempt under this subsection which is  
290 maintained by a covered entity or business associate as  
291 defined in the privacy regulations of the federal Health  
292 Insurance Portability and Accountability Act of 1996 or a  
293 program or qualified service organization as specified in 42  
294 U.S.C. § 290dd-2.

295 (11) Information used for public health activities and  
296 purposes as authorized by the federal Health Insurance  
297 Portability and Accountability Act of 1996, community health  
298 activities, and population health activities.

299 (12) The collection, maintenance, disclosure, sale,  
300 communication, or use of any personal information bearing on a  
301 consumer's credit worthiness, credit standing, credit  
302 capacity, character, general reputation, personal  
303 characteristics, or mode of living by a consumer reporting  
304 agency, furnisher, or user that provides information for use  
305 in a consumer report and by a user of a consumer report, but  
306 only to the extent that the activity is regulated by and  
307 authorized under the federal Fair Credit Reporting Act.

308 (13) Personal data collected, processed, sold, or



## HB351 Enrolled

309 disclosed in compliance with the federal Driver's Privacy  
310 Protection Act of 1994.

311 (14) Personal data regulated by the federal Family  
312 Educational Rights and Privacy Act of 1974.

313 (15) Personal data collected, processed, sold, or  
314 disclosed in compliance with the federal Farm Credit Act of  
315 1971.

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

321 (17) Data processed or maintained as the emergency  
322 contact information of an individual under this act and used  
323 for emergency contact purposes.

324 (18) Data processed or maintained that is necessary to  
325 retain to administer benefits for another individual relating  
326 to the individual who is the subject of the information under  
327 this section and is used for the purposes of administering the  
328 benefits.

329 (19) Personal data collected, processed, sold, or  
330 disclosed in relation to price, route, or service, as these  
331 terms are used in the federal Airline Deregulation Act of 1978  
332 by an air carrier subject to the act.

333 (20) Data or information collected or processed to  
334 comply with or in accordance with state law.

335 (21) Personal data collected or used pursuant to 21  
336 U.S.C. § 830.



## HB351 Enrolled

337 (c) Controllers and processors that comply with the  
338 verifiable parental consent requirements of the federal  
339 Children's Online Privacy Protection Act of 1998 are compliant  
340 with any obligation to obtain parental consent pursuant to  
341 this act.

342 Section 5. (a) Subject to authentication and any other  
343 conditions or limitations provided by this act, a consumer may  
344 invoke the rights authorized pursuant to this subsection at  
345 any time by submitting a request to a controller specifying  
346 the consumer right the consumer seeks to invoke. A controller  
347 shall comply with an authenticated request to do any of the  
348 following:

349 (1) Confirm whether a controller, or a processor or  
350 third party acting on a controller's behalf, is processing the  
351 consumer's personal data and accessing any of the consumer's  
352 personal data under the control of the controller, unless  
353 confirmation or access would require the controller to reveal  
354 a trade secret.

355 (2) Correct inaccuracies in the consumer's personal  
356 data, considering the nature of the personal data and the  
357 purposes of the processing of the consumer's personal data.

358 (3) Direct a controller to delete the consumer's  
359 personal data.

360 (4) Obtain a copy of the consumer's personal data  
361 previously provided by the consumer to a controller in a  
362 portable and, to the extent technically feasible, readily  
363 usable format that allows the consumer to transmit the  
364 personal data to another controller without hindrance when the



## HB351 Enrolled

365 processing is carried out by automated means, unless the  
366 provision of the data would require the controller to reveal a  
367 trade secret.

368 (5) Opt out of the processing of the consumer's  
369 personal data for any of the following purposes:

370 a. Targeted advertising.

371 b. The sale of the consumer's personal data.

372 c. Profiling in furtherance of solely automated  
373 significant decisions concerning the consumer.

374 (b) A controller shall establish a secure and reliable  
375 method for a consumer to exercise rights established by this  
376 section and shall describe the method in the controller's  
377 privacy notice.

378 (c) (1) A parent or legal guardian of a known child may  
379 exercise the consumer's rights on behalf of the known child  
380 regarding the processing of personal data.

381 (2) A guardian or conservator of a consumer may  
382 exercise the consumer's rights on behalf of the consumer  
383 regarding the processing of personal data.

384 (d) Except as otherwise provided in this act, a  
385 controller shall comply with a request by a consumer to  
386 exercise the consumer's rights authorized by this section as  
387 follows:

388 (1)a. A controller shall respond to a consumer's  
389 request within 45 days of receipt of the request.

390 b. A controller may extend the response period by 45  
391 additional days, when reasonably necessary considering the  
392 complexity and number of the consumer's requests, by notifying



## HB351 Enrolled

393 the consumer of the extension and the reason for the extension  
394 within the initial 45-day response period.

395 (2) If a controller declines to act regarding a  
396 consumer's request, the controller shall inform the consumer  
397 of the justification for declining to act within 45 days of  
398 receipt of the request.

399 (3) Information provided in response to a consumer  
400 request must be provided by a controller, free of charge, once  
401 for each consumer during any 12-month period. If a consumer's  
402 requests are manifestly unfounded, excessive, technically  
403 infeasible, or repetitive, the controller may charge the  
404 consumer a reasonable fee to cover the administrative costs of  
405 complying with a request or decline to act on a request. Upon  
406 inquiry by an enforcement authority, the controller bears the  
407 burden of demonstrating the manifestly unfounded, excessive,  
408 technically infeasible, or repetitive nature of a request.

409 (4) If a controller is unable to authenticate a  
410 consumer's request using commercially reasonable efforts, the  
411 controller shall not be required to comply with a request to  
412 initiate an action pursuant to this section and shall provide  
413 notice to the consumer that the controller is unable to  
414 authenticate the request until the consumer provides  
415 additional information reasonably necessary to authenticate  
416 the consumer and the request. A controller is not required to  
417 authenticate an opt-out request, but a controller may deny an  
418 opt-out request if the controller has a good faith,  
419 reasonable, and documented belief that the request is  
420 fraudulent or otherwise not authorized. If a controller denies



## HB351 Enrolled

421 an opt-out request because the controller believes the request  
422 is fraudulent or not authorized, the controller shall send  
423 notice to the person who made the request disclosing that the  
424 controller believes the request is fraudulent or not  
425 authorized and that the controller may not comply with the  
426 request.

427 (5) A controller that has obtained personal data about  
428 a consumer from a source other than the consumer is in  
429 compliance with a consumer's request to delete the consumer's  
430 data if the controller has done either of the following:

431 a. Retained a record of the deletion request and the  
432 minimum data necessary for the purpose of ensuring the  
433 consumer's personal data remains deleted from the controller's  
434 records and refrains from using the retained data for any  
435 other purpose.

436 b. Opted the consumer out of any further processing of  
437 the consumer's personal data for any purpose except for those  
438 exempted pursuant to this act.

439 Section 6. (a) A parent or legal guardian of a known  
440 child or a guardian or conservator of a consumer may act on  
441 the known child's or the consumer's behalf to opt out of the  
442 processing of the known child's or the consumer's personal  
443 data for one or more of the purposes specified in Section 5.

444 (b) A controller must allow a consumer to opt-out by  
445 providing a clear and conspicuous link on the controller's  
446 Internet website to an Internet web page that enables a  
447 consumer directly to opt out of any processing of the  
448 consumer's personal data for the purposes of targeted



## HB351 Enrolled

449 advertising or sale of the consumer's personal data, or  
450 provides up-to-date contact information for a consumer to  
451 submit the opt-out request.

452 (c) (1) If a consumer's decision to opt out of any  
453 processing of the consumer's personal data for the purposes of  
454 targeted advertising, or any sale of personal data, through an  
455 opt-out preference signal sent in accordance with this section  
456 conflicts with the consumer's existing controller-specific  
457 privacy setting or voluntary participation in a controller's  
458 bona fide loyalty, rewards, premium features, discounts, or  
459 club card program, the controller shall comply with the  
460 consumer's opt-out preference signal but may notify the  
461 consumer of the conflict and provide the choice to confirm  
462 controller-specific privacy settings or participation in such  
463 a program.

464 (2) If a controller responds to consumer opt-out  
465 requests received in accordance with this section by informing  
466 the consumer of a charge for the use of any product or  
467 service, the controller shall present the terms of any  
468 financial incentive offered pursuant to this section for the  
469 retention, use, sale, or sharing of the consumer's personal  
470 data.

471 Section 7. (a) A controller shall do all of the  
472 following:

473 (1) Limit the collection of personal data to what is  
474 adequate, relevant, and reasonably necessary in relation to  
475 the purposes for which the personal data is processed.

476 (2) Establish, implement, and maintain reasonable



## HB351 Enrolled

477 administrative, technical, and physical data security  
478 practices to protect the confidentiality, integrity, and  
479 accessibility of personal data appropriate to the volume and  
480 nature of the personal data at issue.

481 (3) Provide an effective mechanism for a consumer to  
482 revoke the consumer's consent under this act that is at least  
483 as easy as the mechanism by which the consumer provided the  
484 consumer's consent and, on revocation of the consent, cease to  
485 further process the personal data as soon as practicable, but  
486 no later than 45 days after complying with the consumer's  
487 opt-out request consistent with this act.

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

489 (1) Except as provided in this act, process personal  
490 data for purposes that are not reasonably necessary to or  
491 compatible with the disclosed purposes for which the personal  
492 data is processed as disclosed by the controller.

493 (2) Process sensitive data concerning a consumer other  
494 than a known child without obtaining that consumer's consent  
495 or, in the case of the processing of personal data concerning  
496 a known child, without processing the data in accordance with  
497 the federal Children's Online Privacy Protection Act of 1998,  
498 15 U.S.C. § 6501 et seq.

499 (3) Process personal data in violation of the laws of  
500 this state or federal laws that prohibit unlawful  
501 discrimination against consumers.

502 (4) Process the personal data of a consumer for the  
503 purposes of targeted advertising or sell a consumer's personal  
504 data without the consumer's consent under circumstances in



## HB351 Enrolled

505 which a controller has actual knowledge that the consumer is  
506 at least 13 years of age but younger than 16 years of age.

507 (5) Deny goods or services, charge different prices or  
508 rates for goods or services, or provide a different level of  
509 quality of goods or services to a consumer if the consumer  
510 opts out of the processing of the consumer's data. However, if  
511 a consumer opts out of data processing, the covered entity is  
512 not required to provide a service that requires data  
513 processing. Controllers may provide different prices or levels  
514 for goods or services if the good or service is a bona fide  
515 loyalty, rewards, premium features, discount, or club card  
516 program in which a consumer voluntarily participates.

517 (c) If a controller sells personal data to third  
518 parties or processes personal data for targeted advertising,  
519 the controller shall clearly and conspicuously disclose the  
520 processing, as well as the way a consumer may exercise the  
521 right to opt out of the processing.

522 (d) A controller shall provide consumers with a  
523 reasonably accurate, clear, and meaningful privacy notice that  
524 includes all of the following:

525 (1) The categories of personal data processed by the  
526 controller.

527 (2) The purpose for processing personal data.

528 (3) The categories of personal data that the controller  
529 shares with third parties, if any.

530 (4) The categories of third parties, if any, with which  
531 the controller shares personal data.

532 (5) An active email address or other mechanism that the



## HB351 Enrolled

533 consumer may use to contact the controller.

534 (6) How consumers may exercise their consumer rights,  
535 including a link or contact information for availing  
536 themselves of the opt-out method provided in Section 6.

537 (e) (1) A controller shall establish and describe in a  
538 privacy notice one or more secure and reliable means for  
539 consumers to submit a request to exercise their consumer  
540 rights, as established under Section 5, pursuant to this act  
541 considering the ways in which consumers normally interact with  
542 the controller, the need for secure and reliable communication  
543 of consumer requests, and the ability of the controller to  
544 authenticate the identity of the consumer or authorized agent  
545 making the request.

546 (2) A controller may not require a consumer to create a  
547 new account to exercise consumer rights but may require a  
548 consumer to use an existing account as a means of exercising  
549 his or her consumer rights.

550 (f) Any provision of a contract or agreement of any  
551 kind that purports to waive or limit in any way a consumer's  
552 consumer rights as established under this act shall be deemed  
553 contrary to public policy and shall be void and unenforceable.

554 Section 8. (a) A processor shall adhere to the  
555 instructions of a controller and shall assist the controller  
556 in meeting the controller's obligations under this act,  
557 considering the nature of processing and the information  
558 available to the processor, including, but not limited to,  
559 both of the following:

560 (1) Maintaining appropriate and reasonably practical



## HB351 Enrolled

561 technical and organizational measures to support the  
562 fulfillment of the controller's obligation to respond to  
563 consumer rights requests.

564 (2) Assisting the controller in meeting the  
565 controller's obligations in relation to the security of  
566 processing the personal data and in relation to the  
567 notification of a breach of security of the system of the  
568 processor to meet both the controller's and the processor's  
569 obligations.

570 (b) (1) A contract between a controller and a processor  
571 shall govern the processor's data processing obligations with  
572 respect to processing performed on behalf of the controller.

573 (2) The contract shall:

574 a. Be binding;

575 b. Clearly set forth instructions for processing data;

576 c. Clearly set forth the nature and purpose of the  
577 processing;

578 d. Clearly set forth the type of data subject to  
579 processing;

580 e. Clearly set forth the duration of processing; and

581 f. Clearly set forth the rights and obligations of both  
582 parties.

583 (3) The contract, taking into account the nature of the  
584 processing, the relationship between the parties, and other  
585 factors, shall also require the processor to:

586 a. Ensure that each processor of personal data is  
587 subject to a duty of confidentiality with respect to the  
588 personal data;



## HB351 Enrolled

589           b. Delete or return all personal data to the controller  
590 as requested at the end of the provision of services at the  
591 controller's direction, unless retention of the personal data  
592 is required or permitted by law or the contract;

593           c. Make available to the controller all information in  
594 the processor's possession necessary to demonstrate the  
595 processor's compliance with the obligations of this act upon  
596 the reasonable request of the controller; and

597           d. Obligate any subcontractor processing personal data  
598 to meet the obligations of the processor with respect to the  
599 personal data.

600           (c) Nothing in this section may be construed to relieve  
601 a controller or processor from the liabilities imposed on the  
602 controller or processor by virtue of the controller's or  
603 processor's role in the processing relationship as described  
604 in this act.

605           (d) Determining whether a person is acting as a  
606 controller or processor with respect to a specific processing  
607 of data is a fact-based determination that depends on the  
608 following context in which personal data is to be processed:

609           (1) A person who is not limited in the processing of  
610 personal data pursuant to a controller's instructions or who  
611 fails to adhere to a controller's instructions is a controller  
612 and not a processor with respect to a specific processing of  
613 data.

614           (2) A processor that continues to adhere to a  
615 controller's instructions with respect to a specific  
616 processing of personal data remains a processor.



## HB351 Enrolled

617 (3) If a processor begins, alone or jointly with  
618 others, determining the purposes and means of the processing  
619 of personal data, the processor is a controller with respect  
620 to the processing and may be subject to an enforcement action  
621 under this act.

622 Section 9. (a) Any controller in possession of  
623 deidentified data shall do all of the following:

624 (1) Take measures to ensure that the deidentified data  
625 cannot reasonably be associated with an individual.

626 (2) Refrain from reidentifying the deidentified data  
627 when maintaining and using deidentified data.

628 (3) Contractually obligate any recipients of the  
629 deidentified data to comply with all provisions of this  
630 section.

631 (b) Nothing in this act may be construed to require a  
632 controller to do any of the following:

633 (1) Reidentify deidentified data or pseudonymous data.

634 (2) Maintain deidentified data in an identifiable form.

635 (3) Collect, obtain, retain, or access any identifiable  
636 data associated with deidentified data solely for purposes of  
637 authenticating a potential consumer request regarding personal  
638 data.

639 (c) Nothing in this act may be construed to require a  
640 controller or processor to comply with an authenticated  
641 consumer rights request if the controller or processor:

642 (1) Is not reasonably capable of associating the  
643 request with the personal data or it would be unreasonably  
644 burdensome to associate the request with the personal data;



## HB351 Enrolled

645 (2) Does not use the personal data to recognize or  
646 respond to the specific consumer who is the subject of the  
647 personal data or associate the personal data with other  
648 personal data about the same specific consumer; and

649 (3) Does not sell the personal data to any third party  
650 or otherwise voluntarily disclose the personal data to any  
651 third party other than a processor or subprocessor, except as  
652 otherwise permitted in this section.

653 (d) The rights afforded under Section 5 may not apply  
654 to pseudonymous data in cases in which the controller is able  
655 to demonstrate that any information necessary to identify the  
656 consumer is kept separately and is subject to effective  
657 technical and organizational controls that prevent the  
658 controller from accessing the information.

659 (e) A controller that discloses pseudonymous data or  
660 deidentified data shall exercise reasonable oversight to  
661 monitor compliance with any contractual commitments to which  
662 the pseudonymous data or deidentified data is subject and  
663 shall take appropriate steps to address any breaches of those  
664 contractual commitments.

665 Section 10. (a) Nothing in this act may be construed to  
666 restrict a controller's or processor's ability to do any of  
667 the following:

668 (1) Comply with federal, state, or local ordinances or  
669 regulations.

670 (2) Comply with a civil, criminal, or regulatory  
671 inquiry, investigation, subpoena, or summons by federal,  
672 state, local, or other government authority.



## HB351 Enrolled

673 (3) Cooperate with law enforcement agencies concerning  
674 conduct or activity that the controller or processor  
675 reasonably and in good faith believes may violate federal,  
676 state, or local ordinances, rules, or regulations.

677 (4) Investigate, establish, exercise, prepare for, or  
678 defend legal claims, or otherwise protect the legal rights of  
679 the controller or processor.

680 (5) Provide a product or service specifically requested  
681 by a consumer.

682 (6) Perform under a contract to which a consumer is a  
683 party, including fulfilling the terms of a written warranty.

684 (7) Take steps at the request of a consumer prior to  
685 entering a contract.

686 (8) Take immediate steps to protect an interest that is  
687 essential for the life or physical safety of the consumer or  
688 another individual and when the processing cannot be  
689 manifestly based on another legal basis.

690 (9) Prevent, detect, protect against, or respond to  
691 security incidents; identify theft, including identity theft,  
692 fraud, harassment, malicious or deceptive activities, or any  
693 illegal activity; preserve the integrity or security of  
694 systems; or investigate, report, or prosecute those  
695 responsible for any of these actions.

696 (10) Engage in public or peer-reviewed scientific or  
697 statistical research in the public interest that adheres to  
698 all other applicable ethics and privacy laws and is approved,  
699 monitored, and governed by an institutional review board that  
700 determines, or similar independent oversight entities that



## HB351 Enrolled

701 determine, all of the following:

702 a. Whether the deletion of the information is likely to  
703 provide substantial benefits that do not exclusively accrue to  
704 the controller.

705 b. The expected benefits of the research outweigh the  
706 privacy risks.

707 c. Whether the controller has implemented reasonable  
708 safeguards to mitigate privacy risks associated with research,  
709 including any risks associated with reidentification.

710 (11) Assist another controller, processor, or third  
711 party with any of the obligations under this act.

712 (12) Process personal data for reasons of public  
713 interest in public health, community health, or population  
714 health, but solely to the extent that the processing is both  
715 of the following:

716 a. Subject to suitable and specific measures to  
717 safeguard the rights of the consumer whose personal data is  
718 being processed.

719 b. Under the responsibility of a professional subject  
720 to confidentiality obligations under federal, state, or local  
721 law.

722 (b) The obligations imposed on controllers or  
723 processors under this act may not restrict a controller's or  
724 processor's ability to collect, use, or retain personal data  
725 for internal use to do any of the following:

726 (1) Conduct internal research to develop, improve, or  
727 repair products, services, or technology.

728 (2) Effectuate a product recall.



## HB351 Enrolled

729 (3) Identify and repair technical errors that impair  
730 existing or intended functionality.

731 (4) Perform internal operations that are reasonably  
732 aligned with the expectations of the consumer or reasonably  
733 anticipated based on the consumer's existing relationship with  
734 the controller or are otherwise compatible with processing  
735 data in furtherance of the provision of a product or service  
736 specifically requested by a consumer or the performance of a  
737 contract to which the consumer is a party.

738 (c) The obligations imposed on controllers or  
739 processors under this act may not apply when compliance by the  
740 controller or processor with this act would violate an  
741 evidentiary privilege under the laws of this state. Nothing in  
742 this act may be construed to prevent a controller or processor  
743 from providing personal data concerning a consumer to a person  
744 covered by an evidentiary privilege under the laws of this  
745 state as part of a privileged communication.

746 (d) (1) If, at the time a controller or processor  
747 discloses personal data to a processor or third-party  
748 controller in accordance with this act, the controller or  
749 processor did not have actual knowledge that the processor or  
750 third-party controller would violate this act, then the  
751 controller or processor may not be considered to have violated  
752 this act.

753 (2) A receiving processor or third-party controller  
754 receiving personal data from a disclosing controller or  
755 processor in compliance with this act is likewise not in  
756 violation of this act for the transgressions of the disclosing



## HB351 Enrolled

757 controller or processor from which the receiving processor or  
758 third-party controller receives the personal data.

759 (e) Nothing in this act may be construed to do either  
760 of the following:

761 (1) Impose any obligation on a controller or processor  
762 that adversely affects the rights or freedoms of any person.

763 (2) Apply to a person's processing of personal data  
764 during the person's personal or household activities.

765 (f) Personal data processed by a controller pursuant to  
766 this section may be processed to the extent that the  
767 processing is both of the following:

768 (1) Reasonably necessary and proportionate to the  
769 purposes listed in this section.

770 (2) Adequate, relevant, and limited to what is  
771 necessary in relation to the specific purposes listed in this  
772 section. The controller or processor must, when applicable,  
773 consider the nature and purpose of the collection, use, or  
774 retention of the personal data collected, used, or retained  
775 pursuant to this section. The personal data must be subject to  
776 reasonable administrative, technical, and physical measures to  
777 protect the confidentiality, integrity, and accessibility of  
778 the personal data and to reduce reasonably foreseeable risks  
779 of harm to consumers relating to the collection, use, or  
780 retention of personal data.

781 (g) If a controller processes personal data pursuant to  
782 an exemption in this section, the controller bears the burden  
783 of demonstrating that the processing qualifies for the  
784 exemption and complies with the requirements in this section.



## HB351 Enrolled

785 (h) Processing personal data for the purposes expressly  
786 identified in this section may not solely make a legal entity  
787 a controller with respect to the processing.

788 Section 11. (a) The Attorney General may enforce  
789 violations of this act.

790 (b) (1) The Attorney General, prior to initiating any  
791 action for a violation of any provision of this act, shall  
792 issue a notice of violation to the controller.

793 (2) If the controller fails to correct the violation  
794 within 45 days after receipt of the notice of violation, the  
795 Attorney General may bring an action for an injunction  
796 pursuant to this section. Upon a finding that the controller  
797 has violated this act and failed to correct the violation as  
798 required by this section, the court may assess a civil penalty  
799 of not more than fifteen thousand dollars (\$15,000) per  
800 violation.

801 (3) If within the 45-day period the controller corrects  
802 the noticed violation and provides the Attorney General an  
803 express written statement that the alleged violations have  
804 been corrected and that no such further violations will occur,  
805 no action may be initiated against the controller.

806 Section 12. This act shall become effective on May 1,  
807 2027.



**HB351 Enrolled**

808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844

---

Speaker of the House of Representatives

---

President and Presiding Officer of the Senate

House of Representatives

I hereby certify that the within Act originated in and was passed by the House 24-Feb-26, as amended.

John Treadwell  
Clerk

Senate	<b>07-Apr-26</b>	Amended and Passed
House	<b>07-Apr-26</b>	Concurred in Senate Amendment