

**SB213 INTRODUCED**



1 SB213  
2 RRIDNMM-1  
3 By Senators Orr, Allen  
4 RFD: Fiscal Responsibility and Economic Development  
5 First Read: 06-Mar-24



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

SYNOPSIS:

Existing law provides for the confidentiality of certain personal information in certain contexts.

This bill would provide that brokers of individual consumers' data must notify consumers of certain information on their website.

This bill would provide that data brokers must register with the Secretary of State.

This bill would provide that data brokers must protect consumers' data through specified security measures.

This bill would require the Secretary of State to adopt rules and procedures to implement and administer the requirements of this bill.

This bill would provide civil penalties for data brokers that violate these notification or registration requirements.

This bill would provide that violations of the duty to protect consumers' data through specified security measures by data brokers constitute violations of the Deceptive Trade Practices Act.

This bill would provide certain persons and information to which the requirements of this bill do not apply.

Section 111.05 of the Constitution of Alabama of



## SB213 INTRODUCED

29           2022, prohibits a general law whose purpose or effect  
30 would be to require a new or increased expenditure of  
31 local funds from becoming effective with regard to a  
32 local governmental entity without enactment by a 2/3  
33 vote unless: it comes within one of a number of  
34 specified exceptions; it is approved by the affected  
35 entity; or the Legislature appropriates funds, or  
36 provides a local source of revenue, to the entity for  
37 the purpose.

38           The purpose or effect of this bill would be to  
39 require a new or increased expenditure of local funds  
40 within the meaning of the section. However, the bill  
41 does not require approval of a local governmental  
42 entity or enactment by a 2/3 vote to become effective  
43 because it comes within one of the specified exceptions  
44 contained in the section.

45  
46  
47  
48  
49  
50

A BILL

TO BE ENTITLED

AN ACT

51           Relating to data privacy; to require consumer data  
52 brokers to publicly state certain information; to require data  
53 brokers to register with the Secretary of State; to require  
54 that data brokers protect data using specified security  
55 measures; to provide civil and criminal penalties for  
56 violations; to provide persons and information to which these



## SB213 INTRODUCED

57 requirements do not apply; and in connection therewith would  
58 have as its purpose or effect the requirement of a new or  
59 increased expenditure of local funds within the meaning of  
60 Section 111.05 of the Constitution of Alabama of 2022.

61 BE IT ENACTED BY THE LEGISLATURE OF ALABAMA:

62 Section 1. For the purposes of this act, the following  
63 terms have the following meanings:

64 (1) BIOMETRIC DATA. Data generated by automatic  
65 measurements of an individual's biological patterns or  
66 characteristics, including fingerprint, voiceprint, retina or  
67 iris scan, information pertaining to an individual's DNA, or  
68 another unique biological pattern or characteristic that is  
69 used to identify a specific individual.

70 (2) CHILD. An individual younger than 13 years of age.

71 (3) COLLECT. In the context of data, means to obtain,  
72 receive, access, or otherwise acquire data by any means,  
73 including by purchasing or renting the data.

74 (4) DATA BROKER. A business entity whose principal  
75 source of revenue is derived from the collecting,  
76 processing, or transferring of personal data that the entity  
77 did not collect directly from the individual linked or  
78 linkable to the data.

79 (5) DE-IDENTIFIED DATA. Data that cannot reasonably be  
80 linked to an identified or identifiable individual or to a  
81 device linked to that individual.

82 (6) EMPLOYEE. An individual who is a director, officer,  
83 staff member, trainee, volunteer, or intern of an employer or  
84 an individual working as an independent contractor for an



## SB213 INTRODUCED

85 employer, regardless of whether the individual is paid,  
86 unpaid, or employed on a temporary basis. The term does not  
87 include an individual contractor who is a service provider.

88 (7) EMPLOYEE DATA. Information collected, processed, or  
89 transferred by an employer if the information satisfies both  
90 of the following:

91 a. Is related to any of the following:

92 1. A job applicant and was collected during the course  
93 of the hiring and application process.

94 2. An employee who is acting in a professional capacity  
95 for the employer, including the employee's business contact  
96 information such as the employee's name, position, title,  
97 business telephone number, business address, or business  
98 e-mail address.

99 3. An employee's emergency contact information.

100 4. An employee or the employee's spouse, dependent,  
101 covered family member, or beneficiary.

102 b. Was collected, processed, or transferred solely for  
103 any of the following:

104 1. A purpose relating to the status of an individual  
105 described by subparagraph a.1. as a current or former job  
106 applicant of the employer.

107 2. A purpose relating to the professional  
108 activities of an employee described by subparagraph a.2. on  
109 behalf of the employer.

110 3. The purpose of having an emergency contact on file  
111 for an employee described by subparagraph a.3. and for  
112 transferring the information in case of an emergency.



## SB213 INTRODUCED

113           4. The purpose of administering benefits  
114 to which an employee described by subparagraph a.4. is  
115 entitled or to which another individual described by that  
116 paragraph is entitled on the basis of the employee's position  
117 with the employer.

118           (8) GENETIC DATA. Any data, regardless of  
119 format, concerning an individual's genetic characteristics.  
120 The term includes raw sequence data derived from sequencing  
121 all or a portion of an individual's extracted DNA and  
122 genotypic and phenotypic information obtained from analyzing  
123 an individual's raw sequence data.

124           (9) KNOWN CHILD. A child under circumstances where a  
125 data broker has actual knowledge of, or willfully disregards  
126 obtaining actual knowledge of, the child's age.

127           (10) PERSONAL DATA. Any information, including  
128 sensitive data, that is linked or reasonably linkable to a  
129 identified or identifiable individual. The term includes  
130 pseudonymous data when the information is used by a controller  
131 or processor in conjunction with additional information that  
132 reasonably links the information to an identified or  
133 identifiable individual. The term does not include  
134 de-identified data, employee data, or publicly available  
135 information.

136           (11) PRECISE GEOLOCATION DATA. Information  
137 accessed on a device or technology that shows the past or  
138 present physical location of an individual or the individual's  
139 device with sufficient precision to identify street-level  
140 location information of the individual or device in a range of



## SB213 INTRODUCED

141 not more than 1,850 feet. The term does not include location  
142 information regarding an individual or device identifiable or  
143 derived solely from the visual content of a legally obtained  
144 image, including the location of a device that captured the  
145 image.

146 (12) PROCESS. In the context of data, an  
147 operation or set of operations performed, whether by manual or  
148 automated means, on personal data or on sets of personal data,  
149 such as the collection, use, storage, disclosure, analysis,  
150 deletion, or modification of personal data.

151 (13) PUBLICLY AVAILABLE INFORMATION. Information to  
152 which any of the following apply:

153 a. Is lawfully made available through governmental  
154 records.

155 b. A business has a reasonable basis to believe  
156 is lawfully available to the general public through widely  
157 distributed media.

158 c. Is lawfully made available by a consumer, or  
159 by an individual to whom a consumer has disclosed the  
160 information, unless the consumer has restricted access to the  
161 information to a specific audience.

162 (14) SENSITIVE DATA.

163 a. A government-issued identifier not required by law  
164 to be publicly available, including any of the following:

- 165 1. A Social Security number.
- 166 2. A passport number.
- 167 3. A driver license number.

168 b. Information that describes or reveals an



## SB213 INTRODUCED

169 individual's mental or physical health diagnosis, condition,  
170 or treatment.

171 c. An individual's financial information, except the  
172 last four digits of a debit or credit card number, including  
173 any of the following:

174 1. A financial account number.

175 2. A credit or debit card number.

176 3. Information that describes or reveals the income  
177 level or bank account balances of the individual.

178 d. Biometric data.

179 e. Genetic data.

180 f. Precise geolocation data.

181 g. An individual's private communication, and that if  
182 made using a device, is not made using a device provided by  
183 the individual's employer that provides conspicuous notice to  
184 the individual that the employer may access communication made  
185 using the device. These communications include, unless the  
186 data broker is the sender or an intended recipient of the  
187 communication, all of the following:

188 1. The individual's voicemails, e-mails, texts, direct  
189 messages, or mail.

190 2. Information that identifies the parties involved in  
191 the communications.

192 3. Information that relates to the transmission of the  
193 communications, including telephone numbers called, telephone  
194 numbers from which calls were placed, the time calls were  
195 made, call duration, and location information of the parties  
196 to the call.





## SB213 INTRODUCED

197 h. A log-in credential, security code, or access code  
198 for an account or device.

199 i. Information identifying the sexual behavior of the  
200 individual in a manner inconsistent with the individual's  
201 reasonable expectation regarding the collection, processing,  
202 or transfer of the information.

203 j. Calendar information, address book information,  
204 phone or text logs, photos, audio recordings, or videos that  
205 are both:

206 1. Maintained for private use by an individual and  
207 stored on the individual's device or in another location.

208 2. Not communicated using a device provided by the  
209 individual's employer unless the employee was provided  
210 conspicuous notice that the employer may access communication  
211 made using the device.

212 k. A photograph, film, video recording, or other  
213 similar medium that shows the individual or a part of the  
214 individual nude or wearing undergarments.

215 1. Information revealing the video content requested or  
216 selected by an individual that is neither of the following:

217 1. Collected by a provider of broadcast television  
218 service, cable service, satellite service, streaming media  
219 service, or other video programming, as that term is defined  
220 by 47 U.S.C. § 613.

221 2. Used solely for transfers for independent video  
222 measurement.

223 m. Information regarding a known child.

224 n. Information revealing an individual's racial or



## SB213 INTRODUCED

225 ethnic origin, color, religious beliefs, or union membership.

226 o. Information identifying an individual's online  
227 activities over time accessing multiple Internet websites or  
228 online services.

229 p. Information collected, processed, or  
230 transferred for the purpose of identifying information  
231 described by this subdivision.

232 (15) SERVICE PROVIDER. A person that receives,  
233 collects, processes, or transfers personal data on behalf of,  
234 and at the direction of, a business or governmental entity,  
235 including a business or governmental entity that is another  
236 service provider, in order for the person to perform a service  
237 or function with or on behalf of the business or governmental  
238 entity.

239 (16) TRANSFER. In the context of data, to disclose,  
240 release, share, disseminate, make available, sell, or license  
241 the data by any means or medium.

242 Section 2. (a) Except as provided by subsection (b),  
243 this act applies to personal data from an individual that is  
244 collected, transferred, or processed by a data broker.

245 (b) This chapter does not apply to any of the following  
246 data:

247 (1) De-identified data, if the data broker does all of  
248 the following:

249 a. Takes reasonable technical measures to ensure that  
250 the data is not able to be used to identify an individual with  
251 whom the data is associated.

252 b. Publicly commits to both of the following in a clear



## SB213 INTRODUCED

253 and conspicuous manner:

254 1. To process and transfer the data solely in a  
255 de-identified form without any reasonable means for  
256 reidentification.

257 2. To not attempt to identify the information to an  
258 individual with whom the data is associated.

259 c. Contractually obligates a person that receives the  
260 information from the provider to both of the following:

261 1. Comply with this subsection with respect to the  
262 information.

263 2. Include those contractual obligations in any  
264 subsequent transfer of the data to another person.

265 (2) Employee data.

266 (3) Publicly available information.

267 (4) Inferences made exclusively from multiple  
268 independent sources of publicly available information that  
269 does not reveal sensitive data with respect to an individual.

270 (5) Data subject to Title V of the Gramm-Leach-Bliley  
271 Act, 15 U.S.C. § 6801, et seq.

272 Section 3. (a) Except as provided by subsection (b),  
273 this act applies only to a data broker that derives either of  
274 the following within a 12-month period:

275 (1) More than 50 percent of the data broker's revenue  
276 from processing or transferring personal data that the data  
277 broker did not collect directly from the individuals to whom  
278 the data pertains.

279 (2) Revenue from processing or transferring the  
280 personal data of more than 50,000 individuals that the data



## SB213 INTRODUCED

281 broker did not collect directly from the individuals to whom  
282 the data pertains.

283 (b) This chapter does not apply to any of the  
284 following:

285 (1) A service provider, including a service provider  
286 that engages in the business of processing employee data for a  
287 third-party employer for the sole purpose of providing  
288 benefits to the third-party employer's employees.

289 (2) A person that collects personal data from another  
290 person to which the person is related by common ownership or  
291 corporate control, provided a reasonable consumer would expect  
292 the persons to share data.

293 (3) A federal, state, tribal, territorial, or local  
294 governmental entity, including a body, authority, board,  
295 bureau, commission, district, agency, or political subdivision  
296 of a governmental entity.

297 (4) An entity that serves as a congressionally  
298 designated nonprofit, national resource center, or  
299 clearinghouse to provide assistance to victims, families,  
300 child-serving professionals, and the general public on missing  
301 and exploited children issues.

302 (5) A consumer reporting agency or other entity that  
303 furnishes information for inclusion in a consumer credit  
304 report or obtains a consumer credit report, but only to the  
305 extent the entity engages in activity regulated or authorized  
306 by the Fair Credit Reporting Act, 15 U.S.C. § 1681, et seq.,  
307 including the collection, maintenance, disclosure, sale,  
308 communication, or use of any personal information bearing on a



## SB213 INTRODUCED

309 consumer's creditworthiness, credit standing, credit capacity,  
310 character, general reputation, personal characteristics, or  
311 mode of living.

312 (6) A financial institution subject to Title V of the  
313 Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, et seq.

314 Section 4. A data broker that maintains an Internet  
315 website or mobile application shall post a conspicuous notice  
316 on the website or application that complies with all of the  
317 following:

318 (1) States that the entity maintaining the website or  
319 application is a data broker.

320 (2) Is clear, not misleading, and readily accessible  
321 by the general public, including individuals with a  
322 disability.

323 (3) Contains language provided by rule of the Secretary  
324 of State for inclusion in the notice.

325 Section 5. (a) To conduct business in this state, a  
326 data broker that is subject to this act shall register by  
327 January 1, 2025, with the Secretary of State by filing a  
328 registration certificate and paying a registration fee of  
329 three hundred dollars (\$300).

330 (b) The registration certificate must include all of  
331 the following:

332 (1) The legal name of the data broker.

333 (2) A contact individual and the primary physical  
334 address, e-mail address, telephone number, and Internet  
335 website address for the data broker.

336 (3) A description of the categories of data the data



## SB213 INTRODUCED

337 broker processes and transfers.

338 (4) A statement of whether or not the data broker  
339 implements a purchaser credentialing process.

340 (5) If the data broker has actual knowledge that the  
341 data broker possesses personal data of a known child, both of  
342 the following:

343 a. A statement detailing the data collection practices,  
344 databases, sales activities, and opt-out policies that are  
345 applicable to the personal data of a known child.

346 b. A statement as to how the data broker complies with  
347 applicable federal and state law regarding the collection,  
348 use, or disclosure of personal data from and about a child on  
349 the Internet.

350 (6) The number of security breaches the data broker has  
351 experienced during the year immediately preceding the year in  
352 which the registration is filed and, if known, the total  
353 number of consumers affected by each breach.

354 (c) The registration certificate may include any  
355 additional information or explanation the data broker chooses  
356 to provide to the Secretary of State concerning the data  
357 broker's data collection practices.

358 (d) A registration certificate expires on the first  
359 anniversary of its date of issuance and every year thereafter.  
360 A data broker may renew a registration certificate by filing a  
361 renewal application, in the form prescribed by the Secretary  
362 of State, and paying a renewal fee of three hundred dollars  
363 (\$300).

364 Section 6. (a) The Secretary of State shall establish



## SB213 INTRODUCED

365 and maintain, on its Internet website, a searchable, central  
366 registry of data brokers registered pursuant to Section 5.

367 (b) The registry must include both of the following:

368 (1) A search feature that allows an individual  
369 searching the registry to identify a specific data broker.

370 (2) For each data broker, the information filed under  
371 Section 5(b).

372 Section 7. (a) A data broker conducting business in  
373 this state has a duty to protect personal data held by the  
374 data broker in accordance with this section.

375 (b) A data broker shall develop, implement, and  
376 maintain a comprehensive information security program that is  
377 written in one or more readily accessible parts and employs  
378 administrative, technical, and physical safeguards that are  
379 appropriate for:

380 (1) The data broker's size, scope, and type of  
381 business;

382 (2) The amount of resources available to the data  
383 broker;

384 (3) The amount of data stored by the data broker; and

385 (4) The need for security and confidentiality of the  
386 personal data stored by the data broker.

387 (c) The comprehensive information security program  
388 required by this section must:

389 (1) Incorporate safeguards that are consistent with the  
390 safeguards for protection of personal data and information of  
391 a similar character under state or federal laws and rules  
392 applicable to the data broker;



## SB213 INTRODUCED

393 (2) Include the designation of one or more employees of  
394 the data broker to maintain the program;

395 (3) Require the identification and assessment of  
396 reasonably foreseeable internal and external risks to the  
397 security, confidentiality, and integrity of any electronic,  
398 paper, or other record containing personal data, and the  
399 establishment of a process for evaluating and improving, as  
400 necessary, the effectiveness of the current safeguards for  
401 limiting those risks, including:

402 a. Requiring ongoing employee and contractor education  
403 and training, including education and training for temporary  
404 employees and contractors of the data broker, on the proper  
405 use of security procedures and protocols and the importance of  
406 personal data security;

407 b. Mandating employee compliance with policies and  
408 procedures established under the program; and

409 c. Providing a means for detecting and preventing  
410 security system failures;

411 (4) Include security policies for the data broker's  
412 employees relating to the storage, access, and transportation  
413 of records containing personal data outside of the broker's  
414 physical business premises;

415 (5) Provide disciplinary measures for violations of a  
416 policy or procedure established under the program;

417 (6) Include measures for preventing a terminated  
418 employee from accessing records containing personal data;

419 (7) Provide policies for the supervision of third-party  
420 service providers that include:





## SB213 INTRODUCED

421 a. Taking reasonable steps to select and retain  
422 third-party service providers that are capable of maintaining  
423 appropriate security measures to protect personal data  
424 consistent with applicable law; and

425 b. Requiring third-party service providers, by  
426 contract, to implement and maintain appropriate security  
427 measures for personal data;

428 (8) Provide reasonable restrictions on physical access  
429 to records containing personal data, including requiring the  
430 records containing the data to be stored in a locked facility,  
431 storage area, or container;

432 (9) Include regular monitoring to ensure that the  
433 program is operating in a manner reasonably calculated to  
434 prevent unauthorized access to or unauthorized use of personal  
435 data and, as necessary, upgrading information safeguards to  
436 limit the risk of unauthorized access to or unauthorized use  
437 of personal data;

438 (10)a. Require the regular review of the scope of the  
439 program's security measures;

440 b. A review of the scope of the program's security  
441 measures must occur at least annually and anytime there is a  
442 material change in the data broker's business practices that  
443 may reasonably affect the security or integrity of records  
444 containing personal data;

445 (11) Require the documentation of responsive actions  
446 taken in connection with any incident involving a breach of  
447 security, including a mandatory post-incident review of each  
448 event and the actions taken, if any, to make changes in



## SB213 INTRODUCED

449 business practices relating to the protection of personal data  
450 in response to that event; and

451 (12) To the extent feasible, include the following  
452 procedures and protocols with respect to computer system  
453 security requirements or procedures and protocols providing a  
454 higher degree of security, for the protection of personal  
455 data:

456 a. Using secure user authentication protocols that  
457 include:

458 1. Controlling user log-in credentials and other  
459 identifiers;

460 2. Using a reasonably secure method of assigning and  
461 selecting passwords or using unique identifier technologies,  
462 which may include biometrics or token devices;

463 3. Controlling data security passwords to ensure that  
464 the passwords are kept in a location and format that do not  
465 compromise the security of the data the passwords protect;

466 4. Restricting access to only active users and active  
467 user accounts; and

468 5. Blocking access to user credentials or  
469 identification after multiple unsuccessful attempts to gain  
470 access;

471 b. Using secure access control measures that include:

472 1. Restricting access to records containing personal  
473 data to only employees or contractors who need access to the  
474 personal data to perform their job duties; and

475 2. Assigning to each employee or contractor with access  
476 to a computer containing personal data a unique identification



## SB213 INTRODUCED

477 and password, which may not be a vendor-supplied default  
478 password, or using another protocol reasonably designed to  
479 maintain the integrity of the security of the access controls  
480 to personal data;

481 c. Encryption of:

482 1. Transmitted records containing personal data that  
483 will travel across public networks; and

484 2. Data containing personal data that is transmitted  
485 wirelessly;

486 d. Reasonable monitoring of systems for unauthorized  
487 use of or access to personal data;

488 e. Encryption of all personal data stored on laptop  
489 computers or other portable devices;

490 f. For records containing personal data on a system  
491 that is connected to the Internet, using reasonably current  
492 firewall protection and operating system security patches that  
493 are reasonably designed to maintain the integrity of the  
494 personal data; and

495 g. Using:

496 1. A reasonably current version of system security  
497 agent software that must include malware protection and  
498 reasonably current patches and virus definitions; or

499 2. A version of system security agent software that is  
500 supportable with current patches and virus definitions and is  
501 set to receive the most current security updates on a regular  
502 basis.

503 (d) A violation of this section by a data broker  
504 constitutes a violation of the Deceptive Trade Practices Act,



## SB213 INTRODUCED

505 Chapter 19 of Title 8, Code of Alabama 1975, and shall be  
506 subject to the same penalties as provided therein.

507 Section 8. (a) A data broker that violates Section 4 or  
508 5 shall be assessed the following civil penalties by the  
509 Secretary of State:

510 (1) One hundred dollars (\$100) for each day the entity  
511 is in violation.

512 (2) The amount of unpaid registration fees for each  
513 year the entity fails to register as required by Section 5.

514 (b) A civil penalty assessed pursuant to this section  
515 may not exceed ten thousand dollars (\$10,000) against a single  
516 data broker during a 12-month period.

517 (c) The Attorney General may bring an action to recover  
518 any civil penalty assessed under this section and may recover  
519 reasonable attorney fees and court costs incurred in bringing  
520 the action.

521 (d) (1) All penalties collected pursuant to this act  
522 shall be deposited into the Consumer Privacy Protection Fund  
523 which is created in the State Treasury. The fund shall be  
524 administered by the Secretary of State for the purpose of  
525 implementing and administering this act.

526 (2) No money shall be withdrawn or expended from this  
527 fund for any purpose unless the monies have been appropriated  
528 by the Legislature and allocated pursuant to this act. Any  
529 monies appropriated shall be budgeted and allocated pursuant  
530 to the Budget Management Act in accordance with Article 4,  
531 commencing with Section 41-4-80 of Chapter 4 of Title 41, Code  
532 of Alabama 1975, and only in the amounts provided by the



## SB213 INTRODUCED

533 Legislature in the general appropriations act or other  
534 appropriations act.

535 Section 9. The Secretary of State shall adopt rules as  
536 necessary to implement this act.

537 Section 10. This act does not apply to the collection,  
538 processing, or transfer of personal data by a data broker  
539 before January 1, 2025.

540 Section 11. Although this bill would have as its  
541 purpose or effect the requirement of a new or increased  
542 expenditure of local funds, the bill is excluded from further  
543 requirements and application under Section 111.05 of the  
544 Constitution of Alabama of 2022, because the bill defines a  
545 new crime or amends the definition of an existing crime.

546 Section 12. This act shall become effective on October  
547 1, 2024.