

Senate Bill 111

By: Senators Albers of the 56th, Burns of the 23rd, Rahman of the 5th, Still of the 48th, Setzler of the 37th and others

A BILL TO BE ENTITLED
AN ACT

1 To amend Title 10 of the Official Code of Georgia Annotated, relating to commerce and
2 trade, so as to enact the "Georgia Consumer Privacy Protection Act"; to protect the privacy
3 of consumer personal data in this state; to provide for definitions; to provide for applicability;
4 to provide for exemptions for certain entities, data, and uses of data; to provide for consumer
5 rights regarding personal data; to provide for a consumer to exercise such rights by
6 submitting a request to a controller; to provide for a controller to promptly respond to such
7 requests; to provide for exemptions; to provide for responsibilities of processors and
8 controllers; to provide for notice and disclosure; to provide for security practices to protect
9 consumer personal data; to allow a controller to offer different goods or services under
10 certain conditions; to provide for limitations; to provide for statutory construction; to provide
11 for enforcement and penalties; to provide an affirmative defense; to prohibit the disclosure
12 of personal data of consumers to local governments unless pursuant to a subpoena or court
13 order; to provide for preemption of local regulation; to provide for related matters; to provide
14 an effective date; to repeal conflicting laws; and for other purposes.

15 BE IT ENACTED BY THE GENERAL ASSEMBLY OF GEORGIA:

16

SECTION 1.

17 Title 10 of the Official Code of Georgia Annotated, relating to commerce and trade, is
18 amended by adding a new article to Chapter 1, relating to selling and other trade practices,
19 to read as follows:

20

"ARTICLE 3721 10-1-960.

22 This article shall be known and may be cited as the 'Georgia Consumer Privacy Protection
23 Act.'

24 10-1-961.25 As used in this article, the term:

26 (1) 'Affiliate' means a legal entity that controls, is controlled by, or is under common
27 control with another legal entity or shares common branding with another legal entity. As
28 used in this paragraph, the term 'control' or 'controlled' means:

29 (A) Ownership of, or the power to vote, more than 50 percent of the outstanding shares
30 of a class of voting security of an entity;

31 (B) Control in any manner over the election of a majority of the directors or of
32 individuals exercising similar functions relative to an entity; or

33 (C) The power to exercise controlling influence over the management of an entity.

34 (2) 'Authenticate' means to verify using reasonable means that a consumer who is
35 entitled to exercise the rights in Code Section 10-1-963, is the same consumer who is
36 exercising such consumer rights with respect to the personal information at issue.

37 (3)(A) 'Biometric data' means data generated by automatic measurement of an
38 individual's biological characteristics, such as a fingerprint, voiceprint, eye retina or iris,

39 or other unique biological patterns or characteristics that are used to identify a specific
40 individual.

41 (B) Such term shall not include:

42 (i) A physical or digital photograph, video recording, or audio recording or data
43 generated from a photograph or video or audio recording;

44 (ii) Information captured and converted to a mathematical representation, including
45 a numeric string or similar configuration, that cannot be used to recreate data
46 generated by automatic measurement of an individual's biological patterns or
47 characteristics used to identify the specific individual; or

48 (iii) Information collected, used, or stored for healthcare treatment, payment, or
49 operations under HIPAA.

50 (4) 'Business associate' shall have the same meaning as provided by HIPAA.

51 (5) 'Consent' means a clear affirmative act signifying a consumer's freely given, specific,
52 informed, and unambiguous agreement to process personal information relating to the
53 consumer. Such term may include a written statement, including a statement written by
54 electronic means, or an unambiguous affirmative action.

55 (6) 'Consumer' means an individual who is a resident of this state acting only in a
56 personal context. Such term shall not include an individual acting in a commercial or
57 employment context.

58 (7) 'Controller' means the person that, alone or jointly with others, determines the
59 purpose and means of processing personal information.

60 (8) 'Covered entity' shall have the same meaning as provided by HIPAA.

61 (9) 'Decisions that produce legal or similarly significant effects concerning the consumer'
62 means decisions made by the controller that result in the provision or denial by the
63 controller of financial or lending services, housing, insurance, education enrollment or
64 opportunity, criminal justice, employment opportunities, healthcare services, or access
65 to basic necessities, such as food and water.

66 (10) 'De-identified data' means data that cannot reasonably be linked to an identified or
67 identifiable individual, or any device linked to such natural person.

68 (11) 'Health record' shall have the same meaning as set forth in paragraph (3) of Code
69 Section 31-33-1. Such term includes the substance of a communication made by an
70 individual to a healthcare facility described in or licensed pursuant to Title 31 in
71 confidence during or in connection with the provision of healthcare services or
72 information otherwise acquired by the healthcare entity about an individual in confidence
73 and in connection with the provision of healthcare services to the individual.

74 (12) 'HIPAA' means the federal Health Insurance Portability and Accountability Act of
75 1996, as amended, 42 U.S.C. Section 1320d et seq.

76 (13) 'Identified or identifiable individual' means a natural person who can be readily
77 identified, whether directly or indirectly.

78 (14) 'Institution of higher education' means a public or private college or university in
79 this state.

80 (15) 'Known child' means an individual who the controller has actual knowledge is under
81 13 years of age.

82 (16) 'NIST' means the National Institute of Standards and Technology privacy
83 framework entitled 'A Tool for Improving Privacy through Enterprise Risk Management
84 Version 1.0' or any subsequent version thereof.

85 (17) 'Nonprofit organization' means an organization exempt from taxation under the
86 Internal Revenue Code, codified in 26 U.S.C. Sections 501-530.

87 (18) 'Person' means any individual or entity.

88 (19) 'Personal information' means information that is linked or reasonably linkable to an
89 identified or identifiable individual. Such term shall not include information that is
90 publicly available or de-identified.

91 (20)(A) 'Precise geolocation data' means information derived from technology,
92 including, but not limited to, global positioning system level latitude and longitude

93 coordinates or other mechanisms, that directly identifies the specific location of a
94 natural person with precision and accuracy within a radius of 1,750 feet.

95 (B) Such term shall not include:

96 (i) The content of communications; or

97 (ii) Data generated by or connected to advanced utility metering infrastructure
98 systems or equipment for use by a utility.

99 (21) 'Process' or 'processing' means an operation or set of operations performed, whether
100 by manual or automated means, on personal information or on sets of personal
101 information, such as the collection, use, storage, disclosure, analysis, deletion, or
102 modification of personal information.

103 (22) 'Processor' means a person that processes personal information on behalf of a
104 controller.

105 (23) 'Profiling' means a form of automated processing performed on personal
106 information solely to evaluate, analyze, or predict personal aspects related to an identified
107 or identifiable individual's economic situation, health, personal preferences, interests,
108 reliability, behavior, location, or movements.

109 (24) 'Protected health information' shall have the same meaning as provided by HIPAA.

110 (25) 'Pseudonymous data' means personal information that cannot be attributed to a
111 specific individual without the use of additional information, so long as the additional
112 information is kept separately and is subject to appropriate technical and organizational
113 measures to ensure that the personal information is not attributed to an identified or
114 identifiable individual.

115 (26) 'Publicly available information' means information that is lawfully made available
116 through federal, state, or local government records, or information that a business has a
117 reasonable basis to believe is lawfully made available to the general public through
118 widely distributed media, by the consumer, or by a person to which the consumer has

119 disclosed the information, unless the consumer has restricted the information to a specific
120 audience.

121 (27)(A) 'Sale of personal information' or 'sell personal information' means the
122 exchange of personal information for monetary or other valuable consideration by the
123 controller to a third party.

124 (B) Such term shall not include:

125 (i) The disclosure of personal information to a processor that processes the personal
126 information on behalf of the controller;

127 (ii) The disclosure of personal information to a third party for purposes of providing
128 a product or service requested by the consumer;

129 (iii) The disclosure or transfer of personal information to an affiliate of the controller;

130 (iv) The disclosure of information that the consumer:

131 (I) Intentionally made available to the general public via a channel of mass media;
132 and

133 (II) Did not restrict to a specific audience; or

134 (v) The disclosure or transfer of personal information to a third party as an asset that
135 is part of a merger, acquisition, bankruptcy, or other transaction in which the third
136 party assumes control of all or part of the controller's assets.

137 (28) 'Sensitive data' means a category of personal information that includes:

138 (A) Personal information revealing racial or ethnic origin, religious belief, mental or
139 physical health diagnosis, sexual orientation, or citizenship or immigration status;

140 (B) The processing of genetic data or biometric data for the purpose of uniquely
141 identifying an individual;

142 (C) The personal information collected from a known child; or

143 (D) Precise geolocation data.

144 (29) 'State agency' means an agency, institution, board, bureau, commission, council, or
145 instrumentality of the executive branch of state government of this state.

146 (30)(A) 'Targeted advertising' means displaying to a consumer an advertisement that
147 is selected based on personal information obtained from such consumer's activities over
148 time and across nonaffiliated websites or online applications to predict the consumer's
149 preferences or interests.

150 (B) Such term shall not include:

151 (i) Advertisements based on activities within a controller's own websites or online
152 applications;

153 (ii) Advertisements based on the context of a consumer's current search query, visit
154 to a website, or online application;

155 (iii) Advertisements directed to a consumer in response to the consumer's request for
156 information or feedback; or

157 (iv) Personal information processed solely for measuring or reporting advertising
158 performance, reach, or frequency.

159 (31) 'Third party' means a person other than the consumer, controller, processor, or an
160 affiliate of the controller or processor.

161 (32) 'Trade secret' shall have the same meaning as set forth in Code Section 16-8-13.

162 10-1-962.

163 (a) This article shall apply to a person that conducts business in this state by producing
164 products or services targeted to consumers of this state that exceeds \$25 million in revenue
165 and that:

166 (1) Controls or processes personal information of at least 25,000 consumers and derives
167 more than 50 percent of gross revenue from the sale of personal information; or

168 (2) During a calendar year, controls or processes personal information of at least 175,000
169 consumers.

170 (b) This article shall not apply to:

171 (1) A person that is:

- 172 (A) A financial institution or an affiliate of a financial institution subject to Title V of
173 the federal Gramm-Leach-Bliley Act, as amended, 15 U.S.C. Section 6801 et seq.;
174 (B) Licensed in this state under Title 33 as an insurance company and transacts
175 insurance business;
176 (C) Licensed in this state under Title 33 as an insurance producer;
177 (D) A covered entity or business associate governed by the privacy, security, and
178 breach notification rules issued by the United States Department of Health and Human
179 Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the federal
180 Health Information Technology for Economic and Clinical Health Act (P.L. 111-5);
181 (E) An air carrier regulated by the secretary of transportation under 49 U.S.C. Section
182 41712 and exempt from state regulations under 49 U.S.C. Section 41713(b)(1); or
183 (F) An entity subject to 42 U.S.C. Section 290dd-2;
184 (2) Data or personal information that is:
185 (A) Subject to Title V of the federal Gramm-Leach-Bliley Act, as amended, 15 U.S.C.
186 Section 6801 et seq.;
187 (B) Protected health information under HIPAA;
188 (C) Considered a health record for purposes of Title 31;
189 (D) Considered patient identifying information for purposes of 42 U.S.C.
190 Section 290dd-2;
191 (E) Processed for purposes of:
192 (i) Research conducted in accordance with the federal policy for the protection of
193 human subjects under 45 C.F.R. Part 46;
194 (ii) Human subjects research conducted in accordance with good clinical practice
195 guidelines issued by the International Council for Harmonization of Technical
196 Requirements for Pharmaceuticals for Human Use; or
197 (iii) Research conducted in accordance with the protection of human subjects under
198 21 C.F.R. Parts 6, 50, and 56;

- 199 (F) Created for purposes of the federal Health Care Quality Improvement Act of 1986,
200 as amended, 42 U.S.C. Section 11101 et seq.;
- 201 (G) Considered patient safety work product for purposes of the federal Patient Safety
202 and Quality Improvement Act, as amended, 42 U.S.C. Section 299b-21 et seq.;
- 203 (H) Derived from the healthcare related information listed in this subsection that is
204 de-identified in accordance with the requirements for de-identification pursuant to
205 HIPAA;
- 206 (I) Included in a limited data set as described in 45 C.F.R. 164.514(e), to the extent that
207 the information is used, disclosed, and maintained in the manner specified in
208 45 C.F.R. 164.514(e);
- 209 (J) Originated from, and intermingled to be indistinguishable with, or information
210 treated in the same manner as, information exempt under this subsection that is
211 maintained by a covered entity or business associate as defined by HIPAA or a program
212 or a qualified service organization as defined by 42 U.S.C. Section 290dd-2;
- 213 (K) Used only for public health activities and purposes as authorized by HIPAA;
- 214 (L) Collected, maintained, disclosed, sold, communicated, or used, bearing upon a
215 consumer's credit worthiness, credit standing, credit capacity, character, general
216 reputation, personal characteristics, or mode of living, by a consumer reporting agency
217 or furnisher that provides information for use in a consumer report, and by a user of a
218 consumer report, but only to the extent that such activity is regulated by and authorized
219 under the federal Fair Credit Reporting Act, as amended, 15 U.S.C. Section 1681 et
220 seq.;
- 221 (M) Collected, processed, or disclosed in compliance with the federal Driver's Privacy
222 Protection Act of 1994, as amended, 18 U.S.C. Section 2721 et seq.;
- 223 (N) Regulated by the federal Family Educational Rights and Privacy Act (FERPA), as
224 amended, 20 U.S.C. Section 1232g et seq.;

225 (O) Collected, processed, or disclosed in compliance with the federal Farm Credit Act,
226 as amended, 12 U.S.C. Section 2001 et seq.; or
227 (P) Maintained or used for purposes of compliance with the regulation of listed
228 chemicals under the federal Controlled Substances Act, as amended, 21 U.S.C.
229 Section 830;
230 (3) Nonprofit organizations that do not sell data;
231 (4) Any state agency, the judicial branch, the legislative branch, or any local government
232 of this state;
233 (5) Any institution of higher education that does not engage in the sale of personal
234 information;
235 (6) Any electric supplier as defined in Code Section 46-3-3 that does not engage in the
236 sale of personal information; or
237 (7) Data processed or maintained:
238 (A) In the course of an individual applying to, being employed by, or acting as an agent
239 or independent contractor of a controller, processor, or third party, to the extent that the
240 data is collected and used within the context of that role;
241 (B) As the emergency contact information of an individual employed by or acting as
242 an agent or independent contractor of a controller, processor, or third party for use as
243 emergency contact purposes with the consent of such individual; or
244 (C) As necessary to retain to administer benefits for an individual who qualifies for
245 benefits as part of the benefits provided to an individual employed by or acting as an
246 agent or independent contractor of a controller, processor, or third party.
247 (c) Controllers and processors that comply with the verifiable parental consent
248 requirements of the federal Children's Online Privacy Protection Act (COPPA), as
249 amended, 15 U.S.C. Section 6501 et seq., shall be deemed compliant with an obligation to
250 obtain parental consent under this article.

251 (d) Nothing in this article shall require a controller, processor, third party, or consumer to
252 disclose trade secrets.

253 10-1-963.

254 (a)(1) A consumer may invoke the consumer rights authorized pursuant to paragraph (2)
255 of this subsection at any time by submitting a request to a controller specifying the
256 consumer rights the consumer wishes to invoke. A known child's parent or legal guardian
257 may invoke the consumer rights authorized pursuant to paragraph (2) of this subsection
258 on behalf of the such known child regarding processing personal information belonging
259 to the known child.

260 (2) A controller shall comply with an authenticated consumer request to exercise the
261 right to:

262 (A) Confirm whether a controller is processing the consumer's personal information
263 and to access such personal information;

264 (B) Correct inaccuracies in the consumer's personal information, taking into account
265 the nature of the personal information and the purposes of the processing of such
266 consumer's personal information;

267 (C) Delete personal information provided by or obtained about the consumer. A
268 controller shall not be required to delete information that it maintains or uses as
269 aggregate or de-identified data; provided, that such data in the possession of the
270 controller is not linked to a specific consumer. A controller that obtained personal
271 information about a consumer from a source other than the consumer shall be in
272 compliance with a consumer's request to delete such personal information by:

273 (i) Retaining a record of the deletion request and the minimum information necessary
274 for the purpose of ensuring that the consumer's personal information remains deleted
275 from the controller's records and by not using such retained personal information for
276 any purpose prohibited under this article; or

277 (ii) Opting the consumer out of the processing of such personal information for any
278 purposes other than those exempted under this article.

279 (D) Obtain a copy of the consumer's personal information that the consumer previously
280 provided to the controller in a portable and, to the extent technically feasible, readily
281 usable format that allows the consumer to transmit such personal information to another
282 controller without hindrance, where the processing is carried out by automated means;
283 or

284 (E) Opt out of a controller's processing of personal information for purposes of:

285 (i) Engaging in the sale of personal information about the consumer;

286 (ii) Targeted advertising; or

287 (iii) Profiling in furtherance of decisions that produce legal or similarly significant
288 effects concerning the consumer.

289 (b) Except as otherwise provided in this article, a controller shall comply with an
290 authenticated request by a consumer to exercise the consumer rights authorized pursuant
291 to paragraph (2) of subsection (a) of this Code section as follows:

292 (1) A controller shall respond to the consumer without undue delay, but in all cases
293 within 45 days of receipt of a request submitted pursuant to subsection (a) of this Code
294 section. The response period may be extended once by 45 additional days when
295 reasonably necessary, taking into account the complexity and number of the consumer's
296 requests, so long as the controller informs the consumer of the extension within the initial
297 45 day response period, together with the reason for the extension;

298 (2) If a controller declines to take action regarding the consumer's request, then the
299 controller shall inform the consumer without undue delay, but in all cases within 45 days
300 of receipt of the request, of the justification for declining to take action and instructions
301 for how to appeal the decision pursuant to subsection (c) of this Code section;

302 (3) Information provided in response to a consumer request shall be provided by a
303 controller free of charge, up to twice annually per consumer. If requests from a consumer

304 are manifestly unfounded, technically infeasible, excessive, or repetitive, then the
305 controller may charge the consumer a reasonable fee to cover the administrative costs of
306 complying with the request or decline to act on the request. The controller bears the
307 burden of demonstrating the manifestly unfounded, technically infeasible, excessive, or
308 repetitive nature of the request; and

309 (4) If a controller is unable to authenticate the request using commercially reasonable
310 efforts, then the controller shall not be required to comply with a request to initiate an
311 action under subsection (a) of this Code section and may request that the consumer
312 provide additional information reasonably necessary to authenticate the consumer and the
313 consumer's request.

314 (c)(1) A controller shall establish a process for a consumer to appeal the controller's
315 refusal to take action on a request within a reasonable period of time after the consumer's
316 receipt of the decision pursuant to paragraph (2) of subsection (b) of this Code section.

317 The appeal process shall be:

318 (A) Made available to the consumer in a conspicuous manner;

319 (B) Available at no cost to the consumer; and

320 (C) Similar to the process for submitting requests to initiate action pursuant to
321 subsection (a) of this Code section.

322 (2) Within 60 days of receipt of an appeal, a controller shall inform the consumer in
323 writing of action taken or not taken in response to the appeal, including a written
324 explanation of the reasons for the decision. If the appeal is denied, the controller shall
325 then also provide the consumer with an online mechanism, if available, or other method
326 through which the consumer may contact the Attorney General to submit a complaint.

327 10-1-964.

328 (a) A controller shall:

- 329 (1) Limit the collection of personal information to what is adequate, relevant, and
330 reasonably necessary in relation to the purposes for which the data is processed, as
331 disclosed to the consumer;
- 332 (2) Except as otherwise provided in this article, not process personal information for
333 purposes that are beyond what is reasonably necessary to and compatible with the
334 disclosed purposes for which the personal information is processed, as disclosed to the
335 consumer, unless the controller obtains the consumer's consent;
- 336 (3) Establish, implement, and maintain reasonable administrative, technical, and physical
337 data security practices, as described in Code Section 10-1-973, to protect the
338 confidentiality, integrity, and accessibility of personal information. The data security
339 practices shall be appropriate to the volume and nature of the personal information at
340 issue;
- 341 (4) Not be required to delete information that it maintains or uses as aggregate or
342 de-identified data, provided that such data in the possession of the business is not linked
343 to a specific consumer;
- 344 (5) Not process personal information in violation of state and federal laws that prohibit
345 unlawful discrimination against consumers. A controller shall not discriminate against
346 a consumer for exercising the consumer rights contained in this article, including denying
347 goods or services, charging different prices or rates for goods or services, or providing
348 a different level of quality of goods and services to the consumer. However, this
349 paragraph shall not require a controller to provide a product or service that requires the
350 personal information of a consumer that the controller does not collect or maintain, or
351 prohibit a controller from offering a different price, rate, level, quality, or selection of
352 goods or services to a consumer, including offering goods or services for no fee, if the
353 consumer has exercised the right to opt out pursuant to subparagraph (E) of paragraph (2)
354 of subsection (a) of Code Section 10-1-963 or the offer is related to a consumer's

355 voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or
356 club card program; and

357 (6) Not process sensitive data concerning a consumer without obtaining the consumer's
358 consent, or, in the case of the processing of sensitive data concerning a known child,
359 without processing the data in accordance with the federal Children's Online Privacy
360 Protection Act, as amended, 15 U.S.C. Section 6501 et seq., and its implementing
361 regulations.

362 (b) A provision of a contract or agreement that purports to waive or limit the consumer
363 rights described in Code Section 10-1-963 is contrary to public policy and is void and
364 unenforceable.

365 (c) A controller shall provide a reasonably accessible, clear, and meaningful privacy notice
366 that includes:

367 (1) The categories of personal information processed by the controller;

368 (2) The purpose for processing personal information;

369 (3) How consumers may exercise their consumer rights pursuant to Code
370 Section 10-1-963, including how a consumer may appeal a controller's decision with
371 regard to the consumer's request;

372 (4) The categories of personal information that the controller sells to third parties, if any;
373 and

374 (5) The categories of third parties, if any, with whom the controller engages in the sale
375 of personal information.

376 (d) If a controller engages in the sale of personal information to third parties or processes
377 personal information for targeted advertising, then the controller shall clearly and
378 conspicuously disclose the processing, as well as the manner in which a consumer may
379 exercise the right to opt out of the processing.

380 (e)(1) A controller shall provide, and shall describe in a privacy notice, one or more
381 secure and reliable means for a consumer to submit a request to exercise the consumer
382 rights described in Code Section 10-1-963. Such means shall take into account the:

383 (A) Ways in which a consumer normally interacts with the controller;

384 (B) Need for secure and reliable communication of such requests; and

385 (C) Ability of a controller to authenticate the identity of the consumer making the
386 request.

387 (2) A controller shall not require a consumer to create a new account in order to exercise
388 the consumer rights described in Code Section 10-1-963, but may require a consumer to
389 use an existing account.

390 10-1-965.

391 (a) A processor shall adhere to the instructions of a controller and shall assist the controller
392 in meeting its obligations under this article. The assistance provided by the processor shall
393 include:

394 (1) Taking into account the nature of processing and the information available to the
395 processor, by appropriate technical and organizational measures, insofar as reasonably
396 practicable, to fulfill the controller's obligation to respond to consumer rights requests
397 pursuant to Code Section 10-1-963; and

398 (2) Providing necessary information to enable the controller to conduct and document
399 data protection assessments pursuant to Code Section 10-1-966.

400 (b) A contract between a controller and a processor governs the processor's data processing
401 procedures with respect to processing performed on behalf of the controller. The contract
402 shall be binding and shall clearly set forth instructions for processing data, the nature and
403 purpose of processing, the type of data subject to processing, the duration of processing,
404 and the rights and obligations of both parties. The contract shall also include requirements
405 that the processor shall:

- 406 (1) Ensure that each person processing personal information is subject to a duty of
407 confidentiality with respect to the data;
- 408 (2) At the controller's direction, delete or return all personal information to the controller
409 as requested at the end of the provision of services, unless retention of the personal
410 information is required by law;
- 411 (3) Upon the reasonable request of the controller, make available to the controller all
412 information in its possession necessary to demonstrate the processor's compliance with
413 the obligations in this article;
- 414 (4) Allow, and cooperate with, reasonable assessments by the controller or the
415 controller's designated assessor; alternatively, the processor may arrange for a qualified
416 and independent assessor to conduct an assessment of the processor's policies and
417 technical and organizational measures in support of the obligations under this article
418 using an appropriate and accepted control standard or framework and assessment
419 procedure for the assessments. The processor shall provide a report of each assessment
420 to the controller upon request; and
- 421 (5) Engage a subcontractor pursuant to a written contract in that requires the
422 subcontractor to meet the obligations of the processor with respect to the personal
423 information.
- 424 (c) Nothing in this Code section shall relieve a controller or a processor from the liabilities
425 imposed on it by virtue of its role in the processing relationship as described in
426 subsection (b) of this Code section.
- 427 (d) Determining whether a person is acting as a controller or processor with respect to a
428 specific processing of data is a fact based determination that depends upon the context in
429 which personal information is to be processed. A processor that continues to adhere to a
430 controller's instructions with respect to a specific processing of personal information
431 remains a processor.

432 10-1-966.

433 (a) A controller shall conduct and document a data protection assessment of each of the
434 following processing activities involving personal information:

435 (1) The processing of personal information for purposes of targeted advertising;

436 (2) The sale of personal information;

437 (3) The processing of personal information for purposes of profiling, where the profiling
438 presents a reasonably foreseeable risk of:

439 (A) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

440 (B) Financial, physical, or reputational injury to consumers;

441 (C) A physical or other intrusion upon the solitude or seclusion, or the private affairs
442 or concerns, of consumers, where the intrusion would be offensive to a reasonable
443 person; or

444 (D) Other substantial injury to consumers;

445 (4) The processing of sensitive data; and

446 (5) Processing activities involving personal information that present a heightened risk
447 of harm to consumers.

448 (b) Data protection assessments conducted pursuant to subsection (a) of this Code section
449 shall identify and weigh the benefits that may flow, directly and indirectly, from the
450 processing to the controller, the consumer, other stakeholders, and the public against the
451 potential risks to the rights of the consumer associated with the processing, as mitigated by
452 safeguards that can be employed by the controller to reduce the risks. The use of
453 de-identified data and the reasonable expectations of consumers, as well as the context of
454 the processing and the relationship between the controller and the consumer whose
455 personal information will be processed, shall be factored into this assessment by the
456 controller.

457 (c) The Attorney General may request pursuant to a civil investigative demand that a
458 controller disclose a data protection assessment that is relevant to an investigation

459 conducted by the Attorney General, and the controller shall make the data protection
460 assessment available to the Attorney General. The Attorney General shall evaluate the data
461 protection assessment for compliance with the responsibilities set forth in Code
462 Section 10-1-964. The disclosure of a data protection assessment pursuant to a request
463 from the Attorney General shall not constitute a waiver of attorney-client privilege or work
464 product protection with respect to the assessment and information contained in the
465 assessment. Such data protection assessments shall be confidential and shall not be open
466 to public inspection and copying under Article 4 of Chapter 18 of Title 50, relating to open
467 records.

468 (d) A single data protection assessment may address a comparable set of processing
469 operations that include similar activities.

470 (e) A data protection assessment conducted by a controller for the purpose of compliance
471 with other laws, rules, or regulations may comply with this Code section if such data
472 protection assessment have a reasonably comparable scope and effect.

473 (f) The data protection assessment requirements in this article shall apply only to
474 processing activities created or generated on or after July 1, 2026.

475 10-1-967.

476 (a) A controller in possession of de-identified data shall:

477 (1) Take reasonable measures to ensure that the data cannot be associated with a natural
478 person;

479 (2) Publicly commit to maintaining and using de-identified data without attempting to
480 reidentify the data; and

481 (3) Contractually obligate recipients of the de-identified data to comply with this article.

482 (b) Nothing in this Code section shall require a controller or processor to:

483 (1) Reidentify de-identified data or pseudonymous data;

484 (2) Maintain data in identifiable form, or collect, obtain, retain, or access data or
485 technology, in order to be capable of associating an authenticated consumer request with
486 personal information; or

487 (3) Comply with an authenticated consumer rights request, pursuant to Code
488 Section 10-1-963, if:

489 (A) The controller is not reasonably capable of associating the request with the
490 personal information or it would be unreasonably burdensome for the controller to
491 associate the request with the personal information;

492 (B) The controller does not use the personal information to recognize or respond to the
493 specific consumer who is the subject of the personal information, or associate the
494 personal information with other personal information about the same specific
495 consumer; and

496 (C) The controller does not engage in the sale of personal information to a third party
497 or otherwise voluntarily disclose the personal information to a third party other than a
498 processor, except as otherwise permitted in this Code section.

499 (c) The consumer rights described in Code Sections 10-1-963 and 10-1-964 shall not apply
500 to pseudonymous data in cases where the controller is able to demonstrate information
501 necessary to identify the consumer is kept separately and is subject to effective technical
502 and organizational controls that prevent the controller from accessing that information.

503 (d) A controller that discloses pseudonymous data or de-identified data shall exercise
504 reasonable oversight to monitor compliance with contractual commitments to which the
505 pseudonymous data or de-identified data is subject and shall take appropriate steps to
506 address breaches of those contractual commitments.

507 10-1-968.

508 (a) Nothing in this article shall restrict a controller's or processor's ability to:

509 (1) Comply with federal, state, or local laws, rules, or regulations;

- 510 (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or
511 summons by federal, state, local, or other governmental authorities;
- 512 (3) Cooperate with law enforcement agencies concerning conduct or activity that the
513 controller or processor reasonably and in good faith believes may violate federal, state,
514 or local laws, rules, or regulations;
- 515 (4) Investigate, establish, exercise, prepare for, or defend legal claims;
- 516 (5) Provide a product or service specifically requested by a consumer or the parent or
517 legal guardian of a known child, perform a contract to which the consumer is a party,
518 including fulfilling the terms of a written warranty, or take steps at the request of the
519 consumer prior to entering into a contract;
- 520 (6) Take immediate steps to protect an interest that is essential for the life or physical
521 safety of the consumer or of another natural person, and where the processing cannot be
522 manifestly based on another legal basis;
- 523 (7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud,
524 harassment, malicious or deceptive activity, or illegal activity; preserve the integrity or
525 security of systems; or investigate, report, or prosecute those responsible for such action;
- 526 (8) Engage in public reviewed or peer reviewed scientific or statistical research in the
527 public interest that adheres to all other applicable ethics and privacy laws and is
528 approved, monitored, and governed by an institutional review board, or similar
529 independent oversight entity that determines whether:
- 530 (A) Deletion of the information is likely to provide substantial benefits that do not
531 exclusively accrue to the controller;
- 532 (B) The expected benefits of the research outweigh the privacy risks; and
- 533 (C) The controller has implemented reasonable safeguards to mitigate privacy risks
534 associated with research, including risks associated with reidentification; or
- 535 (9) Assist another controller, processor, or third party with the obligations under this
536 article.

537 (b) The obligations imposed on controllers or processors under this article shall not restrict
538 a controller's or processor's ability to collect, use, or retain data to:

539 (1) Conduct internal research to develop, improve, or repair products, services, or
540 technology;

541 (2) Effectuate a product recall;

542 (3) Identify and repair technical errors that impair existing or intended functionality;

543 (4) Authenticate an individual for the purpose of allowing access to a secure location or
544 facility; or

545 (5) Perform internal operations that are reasonably aligned with the expectations of the
546 consumer or reasonably anticipated based on the consumer's existing relationship with
547 the controller or are otherwise compatible with processing data in furtherance of the
548 provision of a product or service specifically requested by a consumer or the performance
549 of a contract to which the consumer is a party.

550 (c) The obligations imposed on controllers or processors under this article shall not apply
551 where compliance with this article by the controller or processor would violate an
552 evidentiary privilege under the laws of this state. Nothing in this article shall prevent a
553 controller or processor from providing personal information concerning a consumer to a
554 person covered by an evidentiary privilege under the laws of this state as part of a
555 privileged communication.

556 (d)(1) A controller or processor that discloses personal information to a third-party
557 controller or processor, in compliance with the requirements of this article, shall not be
558 in violation of this article if:

559 (A) The third-party controller or processor that receives and processes the personal
560 information is in violation of this article; and

561 (B) At the time of disclosing the personal information, the disclosing controller or
562 processor did not have actual knowledge that the recipient intended to commit a
563 violation.

564 (2) A third-party controller or processor receiving personal information from a controller
565 or processor in compliance with the requirements of this article is likewise not in
566 violation of this article for the violations of the controller or processor from which it
567 receives such personal information.

568 (e) This article shall not impose an obligation on controllers and processors that adversely
569 affects the rights or freedoms of a person, such as exercising the right of free speech
570 pursuant to the First Amendment to the United States Constitution, or that applies to the
571 processing of personal information by a person in the course of a purely personal activity.

572 (f) A controller shall not process personal information for purposes other than those
573 expressly listed in this Code section unless otherwise allowed by this article. Personal
574 information processed by a controller pursuant to this Code section may be processed to
575 the extent that the processing is:

576 (1) Reasonably necessary and proportionate to the purposes listed in this section; and

577 (2) Adequate, relevant, and limited to what is necessary in relation to the specific
578 purposes listed in this section. Personal information collected, used, or retained pursuant
579 to subsection (b) of this Code section shall, where applicable, take into account the nature
580 and purpose or purposes of the collection, use, or retention. The data shall be subject to
581 reasonable administrative, technical, and physical measures to protect the confidentiality,
582 integrity, and accessibility of the personal information and to reduce reasonably
583 foreseeable risks of harm to consumers relating to the collection, use, or retention of
584 personal information.

585 (g) If a controller processes personal information pursuant to an exemption in this Code
586 section, then the controller bears the burden of demonstrating that the processing qualifies
587 for the exemption and complies with subsection (f) of this Code section.

588 (h) Processing personal information for the purposes expressly identified in any of the
589 paragraphs (1) through (9) of subsection of (a) of this Code section shall not solely make
590 an entity a controller with respect to the processing.

591 10-1-969.

592 Nothing in this article shall be construed to conflict with the specific requirements:

593 (1) Related to the management of health records under Title 31; or

594 (2) Included in federal law.

595 10-1-970.

596 (a) A provision of a contract or agreement that waives or limits a consumer's rights under
597 this article, including, but not limited to, a right to a remedy or means of enforcement, is
598 contrary to public policy, void, and unenforceable.

599 (b) Nothing in this article shall prevent a consumer from declining to request information
600 from a controller, declining to opt out of a controller's sale of the consumer's personal
601 information, or authorizing a controller to sell the consumer's personal information after
602 previously opting out.

603 10-1-971.

604 If the Attorney General has reasonable cause to believe that an individual, controller, or
605 processor has engaged in, is engaging in, or is about to engage in a violation of this article,
606 then the Attorney General may issue a civil investigative demand.

607 10-1-972.

608 (a) The Attorney General shall have exclusive authority to enforce this article.

609 (b) The Attorney General may develop reasonable cause to believe that a controller or
610 processor is in violation of this article, based on the Attorney General's own inquiry or on
611 consumer or public complaints. Prior to initiating an action under this article, the Attorney
612 General shall provide a controller or processor 60 days' written notice identifying the
613 specific provisions of this article the Attorney General alleges have been or are being
614 violated. If within the 60 day period, the controller or processor cures the noticed violation

615 and provides the Attorney General an express written statement that the alleged violations
616 have been cured and that no such further violations shall occur, then the Attorney General
617 shall not initiate an action against the controller or processor.

618 (c) If a controller or processor continues to violate this article following the cure period
619 provided for in subsection (b) of this Code section or breaches an express written statement
620 provided to the Attorney General under subsection (b) of this Code section, then the
621 Attorney General may bring an action in a court of competent jurisdiction seeking any of
622 the following relief:

623 (1) Declaratory judgment that the act or practice violates this article;

624 (2) Injunctive relief, including preliminary and permanent injunctions, to prevent an
625 additional violation of and compel compliance with this article;

626 (3) Civil penalties, as described in subsection (d) of this Code section;

627 (4) Reasonable attorney's fees and investigative costs; or

628 (5) Other relief the court determines appropriate.

629 (d)(1) A court may impose a civil penalty of up to \$7,500.00 for each violation of this
630 article.

631 (2) If the court finds the controller or processor willfully or knowingly violated this
632 article, then the court may, in its discretion, award treble damages.

633 (e) A violation of this article shall not serve as the basis for, or be subject to, a private right
634 of action, including a class action lawsuit, under this article or any other law.

635 (f) The Attorney General may recover reasonable expenses incurred in investigating and
636 preparing a case, including attorney's fees, in an action initiated under this article.

637 10-1-973.

638 (a) A controller or processor shall have an affirmative defense to a cause of action for a
639 violation of this article if the controller or processor creates, maintains, and complies with
640 a written privacy program that:

- 641 (1)(A) Reasonably conforms to the NIST or comparable privacy framework designed
642 to safeguard consumer privacy; and
643 (B) Is updated to reasonably conform with a subsequent revision to the NIST or
644 comparable privacy framework within two years of the publication date stated in the
645 most recent revision to the NIST or comparable privacy framework; and
646 (2) Provides a person with the substantive rights required by this article.
647 (b) The scale and scope of a controller or processor's privacy program under subsection (a)
648 of this Code section shall be appropriate if it is based on all of the following factors:
649 (1) The size and complexity of the controller or processor's business;
650 (2) The nature and scope of the activities of the controller or processor;
651 (3) The sensitivity of the personal information processed;
652 (4) The cost and availability of tools to improve privacy protections and data
653 governance; and
654 (5) Compliance with a comparable state or federal law, if applicable.

655 10-1-974.

- 656 (a) A municipality, county, or consolidated government shall not require a controller or
657 processor to disclose personal information of consumers, unless pursuant to a subpoena or
658 court order.
659 (b) This article shall supersede and preempt any conflicting provisions of any ordinances,
660 resolutions, regulations, or the equivalent adopted by any municipality, county, or
661 consolidated government in this state regarding the processing of personal information by
662 controllers or processors."

663 **SECTION 2.**

664 This Act shall become effective on July 1, 2026, and shall apply to contracts entered into,
665 amended, or renewed on or after such date.

666

SECTION 3.

667 All laws and parts of laws in conflict with this Act are repealed.