

The Senate Committee on Public Safety offered the following substitute to HB 498:

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.

28 For purposes of 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' means a written, printed, or electronically recorded material that:

69 (A) In the course of providing healthcare services to an individual was created or is
70 maintained by a healthcare facility described in or licensed pursuant to Title 31; and

71 (B) Concerns the individual and the healthcare services provided.

72 Such term includes the substance of a communication made by an individual to a
73 healthcare facility described in or licensed pursuant to Title 31 in confidence during or
74 in connection with the provision of healthcare services or information otherwise acquired
75 by the healthcare entity about an individual in confidence and in connection with the
76 provision of healthcare services to the individual.

77 (12) 'HIPAA' means the federal Health Insurance Portability and Accountability Act of
78 1996, as amended, 42 U.S.C. Section 1320d et seq.

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

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

83 (15) 'Known child' means an individual who the controller has actual knowledge is under
84 13 years of age.

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

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

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

91 (19)(A) 'Personal information' means information that is linked or reasonably linkable
92 to an identified or identifiable individual.

- 93 (B) Such term shall not include information that:
- 94 (i) Is publicly available information;
- 95 (ii) Does not identify an individual and with respect to which there is no reasonable
- 96 basis to believe that the information can be used alone or in combination with other
- 97 information to identify an individual; or
- 98 (iii) Is de-identified using a method no less secure than methods provided under
- 99 HIPAA.
- 100 (20)(A) 'Precise geolocation data' means information derived from technology,
- 101 including, but not limited to, global positioning system level latitude and longitude
- 102 coordinates or other mechanisms, that directly identifies the specific location of a
- 103 natural person with precision and accuracy within a radius of 1,750 feet.
- 104 (B) Such term shall not include:
- 105 (i) The content of communications; or
- 106 (ii) Data generated by or connected to advanced utility metering infrastructure
- 107 systems or equipment for use by a utility.
- 108 (21) 'Process' or 'processing' means an operation or set of operations performed, whether
- 109 by manual or automated means, on personal information or on sets of personal
- 110 information, such as the collection, use, storage, disclosure, analysis, deletion, or
- 111 modification of personal information.
- 112 (22) 'Processor' means a person that processes personal information on behalf of a
- 113 controller.
- 114 (23) 'Profiling' means a form of automated processing performed on personal
- 115 information solely to evaluate, analyze, or predict personal aspects related to an identified
- 116 or identifiable individual's economic situation, health, personal preferences, interests,
- 117 reliability, behavior, location, or movements.
- 118 (24) 'Protected health information' shall have the same meaning as provided by HIPAA.

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

124 (26) 'Publicly available information' means information that is lawfully made available
125 through federal, state, or local government records, or information that a business has a
126 reasonable basis to believe is lawfully made available to the general public through
127 widely distributed media, by the consumer, or by a person to which the consumer has
128 disclosed the information, unless the consumer has restricted the information to a specific
129 audience.

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

133 (B) Such term shall not include:

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

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

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

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

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

141 and

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

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

- 146 (28) 'Sensitive data' means a category of personal information that includes:
147 (A) Personal information revealing racial or ethnic origin, religious belief, mental or
148 physical health diagnosis, sexual orientation, or citizenship or immigration status;
149 (B) The processing of genetic data or biometric data for the purpose of uniquely
150 identifying an individual;
151 (C) The personal information collected from a known child; or
152 (D) Precise geolocation data.
- 153 (29) 'State agency' means an agency, institution, board, bureau, commission, council, or
154 instrumentality of the executive branch of state government of this state.
- 155 (30)(A) 'Targeted advertising' means displaying to a consumer an advertisement that
156 is selected based on personal information obtained from such consumer's activities over
157 time and across nonaffiliated websites or online applications to predict the consumer's
158 preferences or interests.
- 159 (B) Such term shall not include:
- 160 (i) Advertisements based on activities within a controller's own websites or online
161 applications;
- 162 (ii) Advertisements based on the context of a consumer's current search query, visit
163 to a website, or online application;
- 164 (iii) Advertisements directed to a consumer in response to the consumer's request for
165 information or feedback; or
- 166 (iv) Personal information processed solely for measuring or reporting advertising
167 performance, reach, or frequency.
- 168 (31) 'Third party' means a person other than the consumer, controller, processor, or an
169 affiliate of the controller or processor.

170 10-1-962.

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

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

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

178 (b) This article shall not apply to:

179 (1) A person that is:

180 (A) A financial institution or an affiliate of a financial institution subject to Title V of
181 the federal Gramm-Leach-Bliley Act, as amended, 15 U.S.C. Section 6801 et seq.;

182 (B) Licensed in this state under Title 33 as an insurance company and transacts
183 insurance business;

184 (C) Licensed in this state under Title 33 as an insurance producer;

185 (D) A covered entity or business associate governed by the privacy, security, and
186 breach notification rules issued by the United States Department of Health and Human
187 Services, 45 C.F.R. Parts 160 and 164 established pursuant to HIPAA, and the federal
188 Health Information Technology for Economic and Clinical Health Act (P.L. 111-5);

189 (E) An air carrier regulated by the secretary of transportation under 49 U.S.C. Section
190 41712 and exempt from state regulations under 49 U.S.C. Section 41713(b)(1); or

191 (F) An entity subject to 42 U.S.C. Section 290dd-2;

192 (2) Data or personal information that is:

193 (A) Subject to Title V of the federal Gramm-Leach-Bliley Act, as amended, 15 U.S.C.
194 Section 6801 et seq.;

195 (B) Protected health information under HIPAA;

196 (C) Considered a health record for purposes of Title 31;

- 197 (D) Considered patient identifying information for purposes of 42 U.S.C.
198 Section 290dd-2;
- 199 (E) Processed for purposes of:
- 200 (i) Research conducted in accordance with the federal policy for the protection of
201 human subjects under 45 C.F.R. Part 46;
- 202 (ii) Human subjects research conducted in accordance with good clinical practice
203 guidelines issued by the International Council for Harmonization of Technical
204 Requirements for Pharmaceuticals for Human Use; or
- 205 (iii) Research conducted in accordance with the protection of human subjects under
206 21 C.F.R. Parts 6, 50, and 56;
- 207 (F) Created for purposes of the federal Health Care Quality Improvement Act of 1986,
208 as amended, 42 U.S.C. Section 11101 et seq.;
- 209 (G) Considered patient safety work product for purposes of the federal Patient Safety
210 and Quality Improvement Act, as amended, 42 U.S.C. Section 299b-21 et seq.;
- 211 (H) Derived from the healthcare related information listed in this subsection that is
212 de-identified in accordance with the requirements for de-identification pursuant to
213 HIPAA;
- 214 (I) Included in a limited data set as described in 45 C.F.R. 164.514(e), to the extent that
215 the information is used, disclosed, and maintained in the manner specified in
216 45 C.F.R. 164.514(e);
- 217 (J) Originated from, and intermingled to be indistinguishable with, or information
218 treated in the same manner as, information exempt under this subsection that is
219 maintained by a covered entity or business associate as defined by HIPAA or a program
220 or a qualified service organization as defined by 42 U.S.C. Section 290dd-2;
- 221 (K) Used only for public health activities and purposes as authorized by HIPAA;
- 222 (L) Impacted a consumer's credit worthiness, credit standing, credit capacity, character,
223 general reputation, personal characteristics, or mode of living by a consumer reporting

224 agency or furnisher that provides information for use in a consumer report, and by a
225 user of a consumer report, but only to the extent that such activity is regulated by and
226 authorized under the federal Fair Credit Reporting Act, as amended, 15 U.S.C.
227 Section 1681 et seq.;
228 (M) Collected, processed, or disclosed in compliance with the federal Driver's Privacy
229 Protection Act of 1994, as amended, 18 U.S.C. Section 2721 et seq.;
230 (N) Regulated by the federal Family Educational Rights and Privacy Act (FERPA), as
231 amended, 20 U.S.C. Section 1232g et seq.;
232 (O) Collected, processed, or disclosed in compliance with the federal Farm Credit Act,
233 as amended, 12 U.S.C. Section 2001 et seq.; or
234 (P) Maintained or used for purposes of compliance with the regulation of listed
235 chemicals under the federal Controlled Substances Act, as amended, 21 U.S.C.
236 Section 830;
237 (3) A nonprofit organization;
238 (4) Any state agency, the judicial branch, the legislative branch, or any local government
239 of this state;
240 (5) Any institution of higher education that does not engage in the sale of personal
241 information;
242 (6) Any electric supplier as defined in Code Section 46-3-3 that does not engage in the
243 sale of personal information; or
244 (7) Data processed or maintained:
245 (A) In the course of an individual applying to, being employed by, or acting as an agent
246 or independent contractor of a controller, processor, or third party, to the extent that the
247 data is collected and used within the context of that role;
248 (B) As the emergency contact information of an individual employed by or acting as
249 an agent or independent contractor of a controller, processor, or third party for use as
250 emergency contact purposes with the consent of such individual; or

251 (C) As necessary to retain to administer benefits for an individual who qualifies for
252 benefits as part of the benefits provided to an individual employed by or acting as an
253 agent or independent contractor of a controller, processor, or third party.

254 (c) Controllers and processors that comply with the verifiable parental consent
255 requirements of the federal Children's Online Privacy Protection Act (COPPA), as
256 amended, 15 U.S.C. Section 6501 et seq., shall be deemed compliant with an obligation to
257 obtain parental consent under this article.

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

260 10-1-963.

261 (a)(1) A consumer may invoke the consumer rights authorized pursuant to paragraph (2)
262 of this subsection at any time by submitting a request to a controller specifying the
263 consumer rights the consumer wishes to invoke. A known child's parent or legal guardian
264 may invoke the consumer rights authorized pursuant to paragraph (2) of this subsection
265 on behalf of the such known child regarding processing personal information belonging
266 to the known child.

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

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

271 (B) Correct inaccuracies in the consumer's personal information, taking into account
272 the nature of the personal information and the purposes of the processing of such
273 consumer's personal information;

274 (C) Delete personal information provided by or obtained about the consumer. A
275 controller shall not be required to delete information that it maintains or uses as
276 aggregate or de-identified data; provided, that such data in the possession of the

277 controller is not linked to a specific consumer. A controller that obtained personal
278 information about a consumer from a source other than the consumer shall be in
279 compliance with a consumer's request to delete such personal information by retaining
280 a record of the deletion request and the minimum information necessary for the purpose
281 of ensuring that the consumer's personal information remains deleted from the
282 controller's records and by not using such retained personal information for any purpose
283 prohibited under this article;

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

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

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

291 (ii) Targeted advertising; or

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

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

297 (1) A controller shall respond to the consumer without undue delay, but in all cases
298 within 45 days of receipt of a request submitted pursuant to subsection (a) of this Code
299 section. The response period may be extended once by 45 additional days when
300 reasonably necessary, taking into account the complexity and number of the consumer's
301 requests, so long as the controller informs the consumer of the extension within the initial
302 45 day response period, together with the reason for the extension;

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

307 (3) Information provided in response to a consumer request shall be provided by a
308 controller free of charge, up to twice annually per consumer. If requests from a consumer
309 are manifestly unfounded, technically infeasible, excessive, or repetitive, then the
310 controller may charge the consumer a reasonable fee to cover the administrative costs of
311 complying with the request or decline to act on the request. The controller bears the
312 burden of demonstrating the manifestly unfounded, technically infeasible, excessive, or
313 repetitive nature of the request; and

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

319 (c) A controller shall establish a process for a consumer to appeal the controller's refusal
320 to take action on a request within a reasonable period of time after the consumer's receipt
321 of the decision pursuant to paragraph (2) of subsection (b) of this Code section. The appeal
322 process shall be:

323 (1) Made available to the consumer in a conspicuous manner;

324 (2) Available at no cost to the consumer; and

325 (3) Similar to the process for submitting requests to initiate action pursuant to
326 subsection (a) of this Code section.

327 Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing
328 of action taken or not taken in response to the appeal, including a written explanation of
329 the reasons for the decision. If the appeal is denied, the controller shall then also provide

330 the consumer with an online mechanism, if available, or other method through which the
331 consumer may contact the Attorney General to submit a complaint.

332 10-1-964.

333 (a) A controller shall:

334 (1) Limit the collection of personal information to what is adequate, relevant, and
335 reasonably necessary in relation to the purposes for which the data is processed, as
336 disclosed to the consumer;

337 (2) Except as otherwise provided in this article, not process personal information for
338 purposes that are beyond what is reasonably necessary to and compatible with the
339 disclosed purposes for which the personal information is processed, as disclosed to the
340 consumer, unless the controller obtains the consumer's consent;

341 (3) Establish, implement, and maintain reasonable administrative, technical, and physical
342 data security practices, as described in Code Section 10-1-973, to protect the
343 confidentiality, integrity, and accessibility of personal information. The data security
344 practices shall be appropriate to the volume and nature of the personal information at
345 issue;

346 (4) Not be required to delete information that it maintains or uses as aggregate or
347 de-identified data, provided that such data in the possession of the business is not linked
348 to a specific consumer;

349 (5) Not process personal information in violation of state and federal laws that prohibit
350 unlawful discrimination against consumers. A controller shall not discriminate against
351 a consumer for exercising the consumer rights contained in this article, including denying
352 goods or services, charging different prices or rates for goods or services, or providing
353 a different level of quality of goods and services to the consumer. However, this
354 paragraph shall not require a controller to provide a product or service that requires the
355 personal information of a consumer that the controller does not collect or maintain, or

356 prohibit a controller from offering a different price, rate, level, quality, or selection of
357 goods or services to a consumer, including offering goods or services for no fee, if the
358 consumer has exercised the right to opt out pursuant to subparagraph (E) of paragraph (2)
359 of subsection (a) of Code Section 10-1-963 or the offer is related to a consumer's
360 voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or
361 club card program; and

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

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

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

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

373 (2) The purpose for processing personal information;

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

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

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

381 (d) If a controller engages in the sale of personal information to third parties or processes
382 personal information for targeted advertising, then the controller shall clearly and

383 conspicuously disclose the processing, as well as the manner in which a consumer may
384 exercise the right to opt out of the processing.

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

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

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

390 (C) Ability of a controller to authenticate the identity of the consumer making the
391 request.

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

395 10-1-965.

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

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

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

405 (b) A contract between a controller and a processor governs the processor's data processing
406 procedures with respect to processing performed on behalf of the controller. The contract
407 shall be binding and shall clearly set forth instructions for processing data, the nature and
408 purpose of processing, the type of data subject to processing, the duration of processing,

409 and the rights and obligations of both parties. The contract shall also include requirements
410 that the processor shall:

411 (1) Ensure that each person processing personal information is subject to a duty of
412 confidentiality with respect to the data;

413 (2) At the controller's direction, delete or return all personal information to the controller
414 as requested at the end of the provision of services, unless retention of the personal
415 information is required by law;

416 (3) Upon the reasonable request of the controller, make available to the controller all
417 information in its possession necessary to demonstrate the processor's compliance with
418 the obligations in this article;

419 (4) Allow, and cooperate with, reasonable assessments by the controller or the
420 controller's designated assessor; alternatively, the processor may arrange for a qualified
421 and independent assessor to conduct an assessment of the processor's policies and
422 technical and organizational measures in support of the obligations under this article
423 using an appropriate and accepted control standard or framework and assessment
424 procedure for the assessments. The processor shall provide a report of each assessment
425 to the controller upon request; and

426 (5) Engage a subcontractor pursuant to a written contract in that requires the
427 subcontractor to meet the obligations of the processor with respect to the personal
428 information.

429 (c) Nothing in this Code section shall relieve a controller or a processor from the liabilities
430 imposed on it by virtue of its role in the processing relationship as described in
431 subsection (b) of this Code section.

432 (d) Determining whether a person is acting as a controller or processor with respect to a
433 specific processing of data is a fact based determination that depends upon the context in
434 which personal information is to be processed. A processor that continues to adhere to a

435 controller's instructions with respect to a specific processing of personal information
436 remains a processor.

437 10-1-966.

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

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

441 (2) The sale of personal information;

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

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

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

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

449 (D) Other substantial injury to consumers;

450 (4) The processing of sensitive data; and

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

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

460 personal information will be processed, shall be factored into this assessment by the
461 controller.

462 (c) The Attorney General may request pursuant to a civil investigative demand that a
463 controller disclose a data protection assessment that is relevant to an investigation
464 conducted by the Attorney General, and the controller shall make the data protection
465 assessment available to the Attorney General. The Attorney General shall evaluate the data
466 protection assessment for compliance with the responsibilities set forth in Code
467 Section 10-1-964. The disclosure of a data protection assessment pursuant to a request
468 from the Attorney General shall not constitute a waiver of attorney-client privilege or work
469 product protection with respect to the assessment and information contained in the
470 assessment. Such data protection assessments shall be confidential and shall not be open
471 to public inspection and copying under Article 4 of Chapter 18 of Title 50, relating to open
472 records.

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

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

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

480 10-1-967.

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

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

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

486 (3) Contractually obligate recipients of the de-identified data to comply with this article.
487 (b) Nothing in this Code section shall require a controller or processor to:
488 (1) Reidentify de-identified data or pseudonymous data;
489 (2) Maintain data in identifiable form, or collect, obtain, retain, or access data or
490 technology, in order to be capable of associating an authenticated consumer request with
491 personal information; or
492 (3) Comply with an authenticated consumer rights request, pursuant to Code
493 Section 10-1-963, if:
494 (A) The controller is not reasonably capable of associating the request with the
495 personal information or it would be unreasonably burdensome for the controller to
496 associate the request with the personal information;
497 (B) The controller does not use the personal information to recognize or respond to the
498 specific consumer who is the subject of the personal information, or associate the
499 personal information with other personal information about the same specific
500 consumer; and
501 (C) The controller does not engage in the sale of personal information to a third party
502 or otherwise voluntarily disclose the personal information to a third party other than a
503 processor, except as otherwise permitted in this Code section.
504 (c) The consumer rights described in Code Sections 10-1-963 and 10-1-964 shall not apply
505 to pseudonymous data in cases where the controller is able to demonstrate information
506 necessary to identify the consumer is kept separately and is subject to effective technical
507 and organizational controls that prevent the controller from accessing that information.
508 (d) A controller that discloses pseudonymous data or de-identified data shall exercise
509 reasonable oversight to monitor compliance with contractual commitments to which the
510 pseudonymous data or de-identified data is subject and shall take appropriate steps to
511 address breaches of those contractual commitments.

512 10-1-968.

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

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

515 (2) Comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or
516 summons by federal, state, local, or other governmental authorities;

517 (3) Cooperate with law enforcement agencies concerning conduct or activity that the
518 controller or processor reasonably and in good faith believes may violate federal, state,
519 or local laws, rules, or regulations;

520 (4) Investigate, establish, exercise, prepare for, or defend legal claims;

521 (5) Provide a product or service specifically requested by a consumer or the parent or
522 legal guardian of a known child, perform a contract to which the consumer is a party,
523 including fulfilling the terms of a written warranty, or take steps at the request of the
524 consumer prior to entering into a contract;

525 (6) Take immediate steps to protect an interest that is essential for the life or physical
526 safety of the consumer or of another natural person, and where the processing cannot be
527 manifestly based on another legal basis;

528 (7) Prevent, detect, protect against, or respond to security incidents, identity theft, fraud,
529 harassment, malicious or deceptive activity, or illegal activity; preserve the integrity or
530 security of systems; or investigate, report, or prosecute those responsible for such action;

531 (8) Engage in public reviewed or peer reviewed scientific or statistical research in the
532 public interest that adheres to all other applicable ethics and privacy laws and is
533 approved, monitored, and governed by an institutional review board, or similar
534 independent oversight entity that determines whether:

535 (A) Deletion of the information is likely to provide substantial benefits that do not
536 exclusively accrue to the controller;

537 (B) The expected benefits of the research outweigh the privacy risks; and

538 (C) The controller has implemented reasonable safeguards to mitigate privacy risks
539 associated with research, including risks associated with reidentification; or

540 (9) Assist another controller, processor, or third party with the obligations under this
541 article.

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

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

546 (2) Effectuate a product recall;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

596 10-1-969.

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

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

599 (2) Included in federal law.

600 10-1-970.

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

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

608 (c) This article shall apply to contracts entered into, amended, or renewed on or after
609 July 1, 2026.

610 10-1-971.

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

614 10-1-972.

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

616 (b) The Attorney General may develop reasonable cause to believe that a controller or
617 processor is in violation of this article, based on the Attorney General's own inquiry or on
618 consumer or public complaints. Prior to initiating an action under this article, the Attorney
619 General shall provide a controller or processor 60 days' written notice identifying the
620 specific provisions of this article the Attorney General alleges have been or are being
621 violated. If within the 60 day period, the controller or processor cures the noticed violation
622 and provides the Attorney General an express written statement that the alleged violations
623 have been cured and that no such further violations shall occur, then the Attorney General
624 shall not initiate an action against the controller or processor.

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

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

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

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

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

635 (5) Other relief the court determines appropriate.

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

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

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

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

644 10-1-973.

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

648 (1)(A) Reasonably conforms to the NIST or comparable privacy framework designed
649 to safeguard consumer privacy; and

650 (B) Is updated to reasonably conform with a subsequent revision to the NIST or
651 comparable privacy framework within two years of the publication date stated in the
652 most recent revision to the NIST or comparable privacy framework; and

653 (2) Provides a person with the substantive rights required by this article.

654 (b) The scale and scope of a controller or processor's privacy program under subsection (a)
655 of this Code section shall be appropriate if it is based on all of the following factors:

656 (1) The size and complexity of the controller or processor's business;

657 (2) The nature and scope of the activities of the controller or processor;

658 (3) The sensitivity of the personal information processed;

659 (4) The cost and availability of tools to improve privacy protections and data
660 governance; and

661 (5) Compliance with a comparable state or federal law, if applicable.

662 10-1-974.

663 (a) A municipality, county, or consolidated government shall not require a controller or
664 processor to disclose personal information of consumers, unless pursuant to a subpoena or
665 court order.

666 (b) This article shall supersede and preempt any conflicting provisions of any ordinances,
667 resolutions, regulations, or the equivalent adopted by any municipality, county, or
668 consolidated government in this state regarding the processing of personal information by
669 controllers or processors."

670 **SECTION 2.**

671 This Act shall become effective on July 1, 2026.

672 **SECTION 3.**

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