

The Senate Committee on Science and Technology offered the following substitute to SB 473:

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; or

44 (ii) Information collected, used, or stored for healthcare treatment, payment, or
45 operations under HIPAA.

46 (4) 'Consent' means a clear affirmative act signifying a consumer's freely given, specific,
47 informed, and unambiguous agreement to process personal information relating to the
48 consumer. Such term may include a written statement, including a statement written by
49 electronic means, or an unambiguous affirmative action.

50 (5) 'Consumer' means an individual who is a resident of this state acting only in a
51 personal context. Such term shall not include an individual acting in a commercial or
52 employment context.

53 (6) 'Controller' means the person that, alone or jointly with others, determines the
54 purpose and means of processing personal information.

55 (7) 'Decisions that produce legal or similarly significant effects concerning the consumer'
56 means decisions made by the controller that result in the provision or denial by the
57 controller of financial or lending services, housing, insurance, education enrollment or
58 opportunity, criminal justice, employment opportunities, healthcare services, or access
59 to basic necessities, such as food and water;

60 (8) 'De-identified data' means data that cannot reasonably be linked to an identified or
61 identifiable individual, or any device linked to such natural person;

62 (9) 'Health record' means a written, printed, or electronically recorded material that:

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

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

66 Such term includes the substance of a communication made by an individual to a
67 healthcare facility described in or licensed pursuant to Title 31 in confidence during or
68 in connection with the provision of healthcare services or information otherwise acquired
69 by the healthcare entity about an individual in confidence and in connection with the
70 provision of healthcare services to the individual.

71 (10) 'HIPAA' means the federal Health Insurance Portability and Accountability Act of
72 1996, as amended, 42 U.S.C. Section 1320d et seq.

73 (11) 'Identified or identifiable individual' means a natural person who can be readily
74 identified, whether directly or indirectly.

75 (12) 'Known child' means an individual who the controller has actual knowledge is under
76 13 years of age.

77 (13) 'NIST' means the National Institute of Standards and Technology privacy
78 framework entitled 'A Tool for Improving Privacy through Enterprise Risk Management
79 Version 1.0.'

80 (14) 'Person' means any individual or entity.

81 (15)(A) 'Personal information' means information that is linked or reasonably linkable
82 to an identified or identifiable individual.

83 (B) Such term shall not include information that:

84 (i) Is publicly available information;

85 (ii) Does not identify an individual and with respect to which there is no reasonable
86 basis to believe that the information can be used alone or in combination with other
87 information to identify an individual; or

88 (iii) Is de-identified using a method no less secure than methods provided under
89 HIPAA.

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

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

94 (B) Such term shall not include:

95 (i) The content of communications; or

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

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

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

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

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

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

119 (22)(A) 'Sale of personal information' means the exchange of personal information for
120 monetary or other valuable consideration by the controller to a third party.

121 (B) Such term shall not include:

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

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

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

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

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

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

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

134 (23) 'Sensitive data' means a category of personal information that includes:

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

137 (B) The processing of genetic data, data that contains 'nudity' or 'sexual conduct' as
138 defined in subsection (b) of Code Section 16-12-181, or biometric data for the purpose
139 of uniquely identifying an individual;

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

141 (D) Precise geolocation data.

142 (24)(A) 'Targeted advertising' means displaying to a consumer an advertisement that
143 is selected based on personal information obtained from such consumer's activities over
144 time and across nonaffiliated public websites or online applications to predict the
145 consumer's preferences or interests.

146 (B) Such term shall not include:

147 (i) Advertisements based on activities within a controller's own public websites or
148 online applications;

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

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

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

155 (25) 'Third party' means a person other than the consumer, controller, processor, or an
156 affiliate of the controller or processor.

157 10-1-962.

158 This article shall apply to a person that conducts business in this state by producing
159 products or services targeted to consumers of this state that exceeds \$25 million in revenue
160 and that:

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

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

165 10-1-963.

166 (a)(1) A consumer may invoke the consumer rights authorized pursuant to paragraph (2)
167 of this subsection at any time by submitting, using a means substantially equivalent to
168 that used by the controller to obtain the consent of the consumer for initial use of the
169 personal information, a request to a controller specifying the consumer rights the
170 consumer wishes to invoke. A known child's parent or legal guardian may invoke the

171 consumer rights authorized pursuant to paragraph (2) of this subsection on behalf of the
172 such known child regarding processing personal information belonging to the known
173 child.

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

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

178 (B) Correct inaccuracies in the consumer's personal information, taking into account
179 the nature of the personal information and the purposes of the processing of such
180 consumer's personal information;

181 (C) Delete personal information provided by or obtained about the consumer. A
182 controller shall not be required to delete information that it maintains or uses as
183 aggregate or de-identified data; provided, that such data in the possession of the
184 controller is not linked to a specific consumer. A controller that obtained personal
185 information about a consumer from a source other than the consumer shall be in
186 compliance with a consumer's request to delete such personal information by retaining
187 a record of the deletion request and the minimum information necessary for the purpose
188 of ensuring that the consumer's personal information remains deleted from the
189 controller's records and by not using such retained personal information for any purpose
190 prohibited under this article;

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

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

197 (i) Selling personal information about the consumer;

198 (ii) Targeted advertising; or
199 (iii) Profiling in furtherance of decisions that produce legal or similarly significant
200 effects concerning the consumer.

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

204 (1) A controller shall respond to the consumer without undue delay, but in all cases
205 within 45 days of receipt of a request submitted pursuant to subsection (a) of this Code
206 section. The response period may be extended once by 45 additional days when
207 reasonably necessary, taking into account the complexity and number of the consumer's
208 requests, so long as the controller informs the consumer of the extension within the initial
209 45 day response period, together with the reason for the extension;

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

214 (3) Information provided in response to a consumer request shall be provided by a
215 controller free of charge, up to twice annually per consumer. If requests from a consumer
216 are manifestly unfounded, technically infeasible, excessive, or repetitive, then the
217 controller may charge the consumer a reasonable fee to cover the administrative costs of
218 complying with the request or decline to act on the request. The controller bears the
219 burden of demonstrating the manifestly unfounded, technically infeasible, excessive, or
220 repetitive nature of the request; and

221 (4) If a controller is unable to authenticate the request using commercially reasonable
222 efforts, then the controller shall not be required to comply with a request to initiate an
223 action under subsection (a) of this Code section and may request that the consumer

224 provide additional information reasonably necessary to authenticate the consumer and the
225 consumer's request.

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

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

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

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

234 Within 60 days of receipt of an appeal, a controller shall inform the consumer in writing
235 of action taken or not taken in response to the appeal, including a written explanation of
236 the reasons for the decision. If the appeal is denied, the controller shall then also provide
237 the consumer with an online mechanism, if available, or other method through which the
238 consumer may contact the Attorney General to submit a complaint.

239 10-1-964.

240 (a) A controller shall:

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

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

248 (3) Establish, implement, and maintain reasonable administrative, technical, and physical
249 data security practices, as described in Code Section 10-1-973, to protect the

250 confidentiality, integrity, and accessibility of personal information. The data security
251 practices shall be appropriate to the volume and nature of the personal information at
252 issue;

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

256 (5) Not process personal information in violation of state and federal laws that prohibit
257 unlawful discrimination against consumers. A controller shall not discriminate against
258 a consumer for exercising the consumer rights contained in this article, including denying
259 goods or services, charging different prices or rates for goods or services, or providing
260 a different level of quality of goods and services to the consumer. However, this
261 paragraph shall not require a controller to provide a product or service that requires the
262 personal information of a consumer that the controller does not collect or maintain, or
263 prohibit a controller from offering a different price, rate, level, quality, or selection of
264 goods or services to a consumer, including offering goods or services for no fee, if the
265 consumer has exercised the right to opt out pursuant to subparagraph (E) of paragraph (2)
266 of subsection (a) of Code Section 10-1-963 or the offer is related to a consumer's
267 voluntary participation in a bona fide loyalty, rewards, premium features, discounts, or
268 club card program; and

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

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

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

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

280 (2) The purpose for processing personal information;

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

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

286 (5) The categories of third parties, if any, to whom the controller sells personal
287 information.

288 (d) If a controller sells personal information to third parties or processes personal
289 information for targeted advertising, then the controller shall clearly and conspicuously
290 disclose the processing, as well as the manner in which a consumer may exercise the right
291 to opt out of the processing.

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

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

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

297 (C) Ability of a controller to authenticate the identity of the consumer making the
298 request.

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

302 10-1-965.

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

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

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

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

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

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

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

326 (4) Allow, and cooperate with, reasonable assessments by the controller or the
327 controller's designated assessor; alternatively, the processor may arrange for a qualified
328 and independent assessor to conduct an assessment of the processor's policies and

329 technical and organizational measures in support of the obligations under this article
330 using an appropriate and accepted control standard or framework and assessment
331 procedure for the assessments. The processor shall provide a report of each assessment
332 to the controller upon request; and

333 (5) Engage a subcontractor pursuant to a written contract in that requires the
334 subcontractor to meet the obligations of the processor with respect to the personal
335 information.

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

339 (d) Determining whether a person is acting as a controller or processor with respect to a
340 specific processing of data is a fact based determination that depends upon the context in
341 which personal information is to be processed. A processor that continues to adhere to a
342 controller's instructions with respect to a specific processing of personal information
343 remains a processor.

344 10-1-966.

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

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

348 (2) The sale of personal information;

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

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

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

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

356 (D) Other substantial injury to consumers;

357 (4) The processing of sensitive data; and

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

360 (b) Data protection assessments conducted pursuant to subsection (a) of this Code section
361 shall identify and weigh the benefits that may flow, directly and indirectly, from the
362 processing to the controller, the consumer, other stakeholders, and the public against the
363 potential risks to the rights of the consumer associated with the processing, as mitigated by
364 safeguards that can be employed by the controller to reduce the risks. The use of
365 de-identified data and the reasonable expectations of consumers, as well as the context of
366 the processing and the relationship between the controller and the consumer whose
367 personal information will be processed, shall be factored into this assessment by the
368 controller.

369 (c) The Attorney General may request pursuant to a civil investigative demand that a
370 controller disclose a data protection assessment that is relevant to an investigation
371 conducted by the Attorney General, and the controller shall make the data protection
372 assessment available to the Attorney General. The Attorney General shall evaluate the data
373 protection assessment for compliance with the responsibilities set forth in Code
374 Section 10-1-964. The disclosure of a data protection assessment pursuant to a request
375 from the Attorney General shall not constitute a waiver of attorney-client privilege or work
376 product protection with respect to the assessment and information contained in the
377 assessment. Such data protection assessments shall be confidential and shall not be open
378 to public inspection and copying under Article 4 of Chapter 18 of Title 50, relating to open
379 records.

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

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

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

387 10-1-967.

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

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

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

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

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

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

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

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

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

404 (B) The controller does not use the personal information to recognize or respond to the
405 specific consumer who is the subject of the personal information, or associate the

406 personal information with other personal information about the same specific
407 consumer; and

408 (C) The controller does not sell the personal information to a third party or otherwise
409 voluntarily disclose the personal information to a third party other than a processor,
410 except as otherwise permitted in this Code section.

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

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

419 10-1-968.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

453 (2) Effectuate a product recall;

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

455 (4) Perform internal operations that are reasonably aligned with the expectations of the
456 consumer or reasonably anticipated based on the consumer's existing relationship with
457 the controller or are otherwise compatible with processing data in furtherance of the

458 provision of a product or service specifically requested by a consumer or the performance
459 of a contract to which the consumer is a party.

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

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

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

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

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

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

482 (f) A controller shall not process personal information for purposes other than those
483 expressly listed in this Code section unless otherwise allowed by this article. Personal

484 information processed by a controller pursuant to this Code section may be processed to
485 the extent that the processing is:

486 (1) Reasonably necessary and proportionate to the purposes listed in this section; and
487 (2) Adequate, relevant, and limited to what is necessary in relation to the specific
488 purposes listed in this section. Personal information collected, used, or retained pursuant
489 to subsection (b) of this Code section shall, where applicable, take into account the nature
490 and purpose or purposes of the collection, use, or retention. The data shall be subject to
491 reasonable administrative, technical, and physical measures to protect the confidentiality,
492 integrity, and accessibility of the personal information and to reduce reasonably
493 foreseeable risks of harm to consumers relating to the collection, use, or retention of
494 personal information.

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

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

501 10-1-969.

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

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

504 (2) Mandated by any provision of federal law.

505 10-1-970.

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

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

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

515 10-1-971.

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

519 10-1-972.

520 (a) The Attorney General may develop reasonable cause to believe that a controller or
521 processor is in violation of this article, based on the Attorney General's own inquiry or on
522 consumer or public complaints. Prior to initiating an action under this article, the Attorney
523 General shall provide a controller or processor 60 days' written notice identifying the
524 specific provisions of this article the Attorney General alleges have been or are being
525 violated. If within the 60 day period, the controller or processor cures the noticed violation
526 and provides the Attorney General an express written statement that the alleged violations
527 have been cured and that no such further violations shall occur, then the Attorney General
528 shall not initiate an action against the controller or processor.

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

- 534 (1) Declaratory judgment that the act or practice violates this article;
535 (2) Injunctive relief, including preliminary and permanent injunctions, to prevent an
536 additional violation of and compel compliance with this article;
537 (3) Civil penalties, as described in subsection (c) of this Code section;
538 (4) Reasonable attorney's fees and investigative costs; or
539 (5) Other relief the court determines appropriate.

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

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

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

546 10-1-973.

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

550 (1)(A) Reasonably conforms to the NIST procedures designed to safeguard consumer
551 privacy; and

552 (B) Is updated to reasonably conform with a subsequent revision to the NIST within
553 two years of the publication date stated in the most recent revision to the NIST; and

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

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

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

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

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

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

562 (5) Compliance with a comparable state or federal law.

563 10-1-974.

564 (a) A municipality, county, or consolidated government shall not require a controller or
565 processor to disclose personal data of consumers, unless pursuant to a subpoena or court
566 order.

567 (b) This article shall supersede and preempt any conflicting provisions of any ordinances,
568 resolutions, regulations, or the equivalent adopted by any municipality, county, or
569 consolidated government regarding the processing of personal data by controllers or
570 processors."

571 **SECTION 2.**

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

573 **SECTION 3.**

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