General Assembly

Substitute Bill No. 893

AN ACT CONCERNING CONSUMER PRIVACY.

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1   Section 1. (NEW) (*Effective January 1, 2023*) As used in this section and
2   sections 2 to 11, inclusive, of this act, unless the context otherwise
3   requires:

4   (1) "Affiliate" means a legal entity that controls, is controlled by, or is
5   under common control with another legal entity or shares common
6   branding with another legal entity. For the purposes of this subdivision,
7   "control" or "controlled" means (A) ownership of, or the power to vote,
8   more than fifty per cent of the outstanding shares of any class of voting
9   security of a company, (B) control in any manner over the election of a
10   majority of the directors or of individuals exercising similar functions,
11   or (C) the power to exercise controlling influence over the management
12   of a company.

13   (2) "Authenticate" means to verify through reasonable means that the
14   consumer is the same consumer exercising such consumer rights with
15   respect to the personal data at issue.

16   (3) "Biometric data" means data generated by automatic
17   measurements of an individual's biological characteristics, such as a
18   fingerprint, voiceprint, eye retinas, irises or other unique biological

19 patterns or characteristics that are used to identify a specific individual.
20 "Biometric data" does not include a physical or digital photograph, a
21 video or audio recording or data generated therefrom, or information
22 collected, used or stored for health care treatment, payment or
23 operations under HIPAA.

24 (4) "Business associate" has the same meaning as provided in HIPAA.

25 (5) "Child" means any natural person less than thirteen years of age.

26 (6) "Consent" means a clear affirmative act signifying a consumer's
27 freely given, specific, informed and unambiguous agreement to allow
28 the processing of personal data relating to the consumer. "Consent" may
29 include a written statement, including by electronic means, or any other
30 unambiguous affirmative action.

31 (7) "Consumer" means a natural person who is a resident of this state
32 and acting only in an individual or household context. "Consumer" does
33 not include a natural person acting in a commercial or employment
34 context.

35 (8) "Controller" means a natural or legal person that, alone or jointly
36 with others, determines the purpose and means of processing personal
37 data.

38 (9) "Covered entity" has the same meaning as provided in HIPAA.

39 (10) "Decisions that produce legal or similarly significant effects
40 concerning a consumer" means decisions made by the controller that
41 result in the provision or denial by the controller of financial and
42 lending services, housing, insurance, education enrollment, criminal
43 justice, employment opportunities, health care services or access to basic
44 necessities, such as food and water.

45 (11) "De-identified data" means data that cannot reasonably be linked
46 to an identified or identifiable natural person, or a device linked to such
47 person.

48   (12) "Health record" means the health-related record of an individual,
49 and may include, but need not be limited to, continuity of care
50 documents, discharge summaries and other information or data relating
51 to a patient's demographics, medical history, medication, allergies,
52 immunizations, laboratory test results, radiology or other diagnostic
53 images, vital signs and statistics.

54   (13) "Health care provider" means any person, corporation, limited
55 liability company, facility or institution licensed by this state to provide
56 health care or professional services, or an officer, employee or agent
57 thereof acting in the course and scope of his or her employment.

58   (14) "HIPAA" means the Health Insurance Portability and
59 Accountability Act of 1996, 42 USC 1320d et seq.

60   (15) "Identified or identifiable natural person" means a person who
61 can be readily identified, directly or indirectly.

62   (16) "Institution of higher education" means any person, school,
63 board, association, limited liability company or corporation that is
64 licensed or accredited to offer one or more programs of higher learning
65 leading to one or more degrees.

66   (17) "Nonprofit organization" means any organization that is exempt
67 from taxation under Section 501(c)(3) of the Internal Revenue Code of
68 1986, or any subsequent corresponding internal revenue code of the
69 United States, as amended from time to time.

70   (18) "Personal data" means any information that is linked or
71 reasonably linkable to an identified or identifiable natural person.
72 "Personal data" does not include de-identified data or publicly available
73 information.

74   (19) "Precise geolocation data" means information derived from
75 technology, including, but not limited to, global positioning system
76 level latitude and longitude coordinates or other mechanisms, that
77 directly identify the specific location of a natural person with precision

78 and accuracy within a radius of one thousand seven hundred fifty feet.
79 "Precise geolocation data" does not include the content of
80 communications or any data generated by or connected to advanced
81 utility metering infrastructure systems or equipment for use by a utility.

82   (20) "Process" or "processing" means any operation or set of
83 operations performed, whether by manual or automated means, on
84 personal data or on sets of personal data, such as the collection, use,
85 storage, disclosure, analysis, deletion or modification of personal data.

86   (21) "Processor" means a natural or legal entity that processes
87 personal data on behalf of a controller.

88   (22) "Profiling" means any form of automated processing performed
89 on personal data to evaluate, analyze, or predict personal aspects related
90 to an identified or identifiable natural person's economic situation,
91 health, personal preferences, interests, reliability, behavior, location or
92 movements.

93   (23) "Protected health information" has the same meaning as
94 provided in HIPAA.

95   (24) "Pseudonymous data" means personal data that cannot be
96 attributed to a specific natural person without the use of additional
97 information, provided that such additional information is kept
98 separately and is subject to appropriate technical and organizational
99 measures to ensure that the personal data is not attributed to an
100 identified or identifiable natural person.

101   (25) "Publicly available information" means information that is
102 lawfully made available through federal, state or municipal government
103 records, or information that a business has a reasonable basis to believe
104 is lawfully made available to the general public through widely
105 distributed media, by the consumer, or by a person to whom the
106 consumer has disclosed the information, unless the consumer has
107 restricted the information to a specific audience.

108 (26) "Sale of personal data" means the exchange of personal data for
109 monetary consideration by the controller to a third party. "Sale of
110 personal data" does not include: (A) The disclosure of personal data to
111 a processor that processes the personal data on behalf of the controller,
112 (B) the disclosure of personal data to a third party for purposes of
113 providing a product or service requested by the consumer, (C) the
114 disclosure or transfer of personal data to an affiliate of the controller, (D)
115 the disclosure of information that the consumer (i) intentionally made
116 available to the general public via a channel of mass media, and (ii) did
117 not restrict to a specific audience, or (E) the disclosure or transfer of
118 personal data to a third party as an asset that is part of a merger,
119 acquisition, bankruptcy or other transaction in which the third party
120 assumes control of all or part of the controller's assets.

121 (27) "Sensitive data" means personal data that includes: (A) Data
122 revealing racial or ethnic origin, religious beliefs, mental or physical
123 health diagnosis, sexual orientation or citizenship or immigration
124 status, (B) the processing of genetic or biometric data for the purpose of
125 uniquely identifying a natural person, (C) personal data collected from
126 a known child, or (D) precise geolocation data.

127 (28) "Targeted advertising" means displaying advertisements to a
128 consumer where the advertisement is selected based on personal data
129 obtained from that consumer's activities over time and across
130 nonaffiliated Internet web sites or online applications to predict such
131 consumer's preferences or interests. "Targeted advertising" does not
132 include: (A) Advertisements based on activities within a controller's
133 own Internet web sites or online applications, (B) advertisements based
134 on the context of a consumer's current search query, visit to an Internet
135 web site or online application, (C) advertisements directed to a
136 consumer in response to the consumer's request for information or
137 feedback, or (D) the processing of personal data solely for measuring or
138 reporting advertising performance, reach or frequency.

139 (29) "Third party" means a natural or legal person, public authority,
140 agency or body other than the consumer, controller, processor or an

141 affiliate of the processor or the controller.

142 Sec. 2. (NEW) (*Effective January 1, 2023*) The provisions of sections 1
143 to 11, inclusive, of this act apply to persons that conduct business in this
144 state or persons that produce products or services that are targeted to
145 residents of this state and that: (1) During a calendar year, control or
146 process the personal data of not less than one hundred thousand
147 consumers, or (2) control or process the personal data of not less than
148 twenty-five thousand consumers and derive more than fifty per cent of
149 their gross revenue from the sale of personal data.

150 Sec. 3. (NEW) (*Effective January 1, 2023*) (a) The provisions of sections
151 1 to 11, inclusive, of this act shall not apply to any: (1) Body, authority,
152 board, bureau, commission, district or agency of this state or of any
153 political subdivision of this state, (2) financial institution or data subject
154 to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq., (3)
155 covered entity or business associate governed by the privacy, security
156 and breach notification rules issued by the United States Department of
157 Health and Human Services, 45 CFR 160 and 164, established pursuant
158 to HIPAA, and the Health Information Technology for Economic and
159 Clinical Health Act, (4) nonprofit organization, or (5) institution of
160 higher education.

161 (b) The following information and data is exempt from the provisions
162 of sections 1 to 11, inclusive, of this act: (1) Protected health information
163 under HIPAA, (2) health records, (3) patient identifying information for
164 purposes of 42 USC 290dd-2, (4) identifiable private information for
165 purposes of the federal policy for the protection of human subjects
166 under 45 CFR 46, (5) identifiable private information that is otherwise
167 information collected as part of human subjects research pursuant to the
168 good clinical practice guidelines issued by the International Council for
169 Harmonization of Technical Requirements for Pharmaceuticals for
170 Human Use, (6) the protection of human subjects under 21 CFR 6, 50
171 and 56, or personal data used or shared in research, as defined in 45 CFR
172 164.501, that is conducted in accordance with the standards set forth in
173 this subdivision and subdivisions (4) and (5) of this subsection, or other

174 research conducted in accordance with applicable law, (7) information
175 and documents created for purposes of the Health Care Quality
176 Improvement Act of 1986, 42 USC 11101 et seq., (8) patient safety work
177 product for purposes of the Patient Safety and Quality Improvement
178 Act, 42 USC 299b-21 et seq., (9) information derived from any of the
179 health care related information listed in this subsection that is de-
180 identified in accordance with the requirements for de-identification
181 pursuant to HIPAA, (10) information originating from, and
182 intermingled to be indistinguishable with, or information treated in the
183 same manner as information exempt under this subsection that is
184 maintained by a covered entity or business associate, program or
185 qualified service organization, as specified in 42 USC 290dd-2, (11)
186 information used for public health activities and purposes as authorized
187 by HIPAA, (12) the collection, maintenance, disclosure, sale,
188 communication or use of any personal information bearing on a
189 consumer's credit worthiness, credit standing, credit capacity, character,
190 general reputation, personal characteristics or mode of living by a
191 consumer reporting agency, furnisher or user that provides information
192 for use in a consumer report, and by a user of a consumer report, but
193 only to the extent that such activity is regulated by and authorized
194 under the Fair Credit Reporting Act, 15 USC 1681 et seq., (13) personal
195 data collected, processed, sold or disclosed in compliance with the
196 Driver's Privacy Protection Act of 1994, 18 USC 2721 et seq., (14)
197 personal data regulated by the Family Educational Rights and Privacy
198 Act, 20 USC 1232g et seq., (15) personal data collected, processed, sold
199 or disclosed in compliance with the Farm Credit Act, 12 USC 2001 et
200 seq., and (16) data processed or maintained (A) in the course of an
201 individual applying to, employed by, or acting as an agent or
202 independent contractor of, a controller, processor or third party, to the
203 extent that the data is collected and used within the context of that role;
204 (B) as the emergency contact information of an individual under
205 sections 1 to 11, inclusive, of this act used for emergency contact
206 purposes, or (C) that is necessary to retain to administer benefits for
207 another individual relating to the individual under subdivision (1) of
208 this subsection and used for the purposes of administering such

209 benefits.

210 (c) Controllers and processors that comply with the verifiable
211 parental consent requirements of the Children's Online Privacy
212 Protection Act, 15 USC 6501 et seq., shall be deemed compliant with any
213 obligation to obtain parental consent pursuant to sections 1 to 11,
214 inclusive, of this act.

215 Sec. 4. (NEW) (*Effective January 1, 2023*) (a) A consumer may invoke
216 the consumer rights authorized pursuant to this section at any time by
217 submitting a request to a controller specifying the consumer rights the
218 consumer wishes to invoke. A known child's parent or legal guardian
219 may invoke such consumer rights on behalf of the child regarding
220 processing personal data belonging to the known child. A controller
221 shall comply with an authenticated consumer request to exercise the
222 right to: (1) Confirm whether or not a controller is processing the
223 consumer's personal data and to access such personal data, (2) correct
224 inaccuracies in the consumer's personal data, taking into account the
225 nature of the personal data and the purposes of the processing of the
226 consumer's personal data, (3) delete personal data provided by, or
227 obtained about, the consumer, (4) obtain a copy of the consumer's
228 personal data that the consumer previously provided to the controller
229 in a portable and, to the extent technically feasible, readily usable format
230 that allows the consumer to transmit the data to another controller
231 without hindrance, where the processing is carried out by automated
232 means, and (5) opt out of the processing of the personal data for
233 purposes of (A) targeted advertising, (B) the sale of personal data, or (C)
234 profiling in furtherance of decisions that produce legal or similarly
235 significant effects concerning the consumer.

236 (b) Except as otherwise provided in sections 1 to 11, inclusive, of this
237 act, a controller shall comply with a request by a consumer to exercise
238 the consumer rights authorized pursuant to said sections as follows:

239 (1) A controller shall respond to the consumer without undue delay,
240 but not later than forty-five days after receipt of the request. The

241 response period may be extended once by forty-five additional days
242 when reasonably necessary, considering the complexity and number of
243 the consumer's requests, provided the controller informs the consumer
244 of any such extension within the initial forty-five-day response period,
245 together with the reason for the extension.

246   (2) If a controller declines to take action regarding the consumer's
247 request, the controller shall inform the consumer without undue delay,
248 but not later than forty-five days after receipt of the request, of the
249 justification for declining to take action and instructions for how to
250 appeal the decision.

251   (3) Information provided in response to a consumer request shall be
252 provided by a controller free of charge, up to twice annually per
253 consumer. If requests from a consumer are manifestly unfounded,
254 excessive or repetitive, the controller may charge the consumer a
255 reasonable fee to cover the administrative costs of complying with the
256 request or decline to act on the request. The controller bears the burden
257 of demonstrating the manifestly unfounded, excessive or repetitive
258 nature of the request.

259   (4) If a controller is unable to authenticate the request using
260 commercially reasonable efforts, the controller shall not be required to
261 comply with a request to initiate an action pursuant to this section and
262 may request that the consumer provide additional information
263 reasonably necessary to authenticate the consumer and the consumer's
264 request.

265   (c) A controller shall establish a process for a consumer to appeal the
266 controller's refusal to take action on a request within a reasonable period
267 of time after the consumer's receipt of the decision. The appeal process
268 shall be conspicuously available and similar to the process for
269 submitting requests to initiate action pursuant to this section. Not later
270 than sixty days after receipt of an appeal, a controller shall inform the
271 consumer in writing of any action taken or not taken in response to the
272 appeal, including a written explanation of the reasons for the decisions.

273 If the appeal is denied, the controller shall also provide the consumer
274 with an online mechanism, if available, or other method through which
275 the consumer may contact the Attorney General to submit a complaint.

276   Sec. 5. (NEW) (*Effective January 1, 2023*) (a) A controller shall: (1) Limit
277 the collection of personal data to what is adequate, relevant and
278 reasonably necessary in relation to the purposes for which such data is
279 processed, as disclosed to the consumer, (2) except as otherwise
280 provided in sections 1 to 11, inclusive, of this act, not process personal
281 data for purposes that are neither reasonably necessary to nor
282 compatible with the disclosed purposes for which such personal data is
283 processed, as disclosed to the consumer, unless the controller obtains
284 the consumer's consent, (3) establish, implement and maintain
285 reasonable administrative, technical and physical data security practices
286 to protect the confidentiality, integrity and accessibility of personal data
287 appropriate to the volume and nature of the personal data at issue, (4)
288 not process sensitive data concerning a consumer without obtaining the
289 consumer's consent, or, in the case of the processing of sensitive data
290 concerning a known child, without processing such data in accordance
291 with the federal Children's Online Privacy Protection Act, 15 USC 6501
292 et seq., and (5) not process personal data in violation of the laws of this
293 state and federal laws that prohibit unlawful discrimination against
294 consumers. A controller shall not discriminate against a consumer for
295 exercising any of the consumer rights contained in sections 1 to 11,
296 inclusive, of this act, including denying goods or services, charging
297 different prices or rates for goods or services or providing a different
298 level of quality of goods and services to the consumer. Nothing in this
299 subsection shall be construed to require a controller to provide a
300 product or service that requires the personal data of a consumer that the
301 controller does not collect or maintain or to prohibit a controller from
302 offering a different price, rate, level, quality or selection of goods or
303 services to a consumer, including offering goods or services for no fee,
304 if the consumer has exercised his right to opt out or the offer is related
305 to a consumer's voluntary participation in a bona fide loyalty, rewards,
306 premium features, discounts or club card program.

307   (b) Controllers shall provide consumers with a reasonably accessible,
308   clear, and meaningful privacy notice that includes: (1) The categories of
309   personal data processed by the controller, (2) the purpose for processing
310   personal data, (3) how consumers may exercise their consumer rights,
311   including how a consumer may appeal a controller's decision with
312   regard to the consumer's request, (4) the categories of personal data that
313   the controller shares with third parties, if any, and (5) the categories of
314   third parties, if any, with which the controller shares personal data.

315   (c) If a controller sells personal data to third parties or processes
316   personal data for targeted advertising, the controller shall clearly and
317   conspicuously disclose such processing, as well as the manner in which
318   a consumer may exercise the right to opt out of such processing.

319   (d) A controller shall establish, and shall describe in a privacy notice,
320   one or more secure and reliable means for consumers to submit a
321   request to exercise their consumer rights pursuant to sections 1 to 11,
322   inclusive, of this act. Such means shall take into account the ways in
323   which consumers normally interact with the controller, the need for
324   secure and reliable communication of such requests, and the ability of
325   the controller to authenticate the identity of the consumer making the
326   request. Controllers shall not require a consumer to create a new account
327   in order to exercise consumer rights, but may require a consumer to use
328   an existing account.

329   Sec. 6. (NEW) (*Effective January 1, 2023*) (a) A processor shall adhere
330   to the instructions of a controller and shall assist the controller in
331   meeting its obligations pursuant to sections 1 to 11, inclusive, of this act.
332   Such assistance shall include: (1) Taking into account the nature of
333   processing and the information available to the processor, by
334   appropriate technical and organizational measures, insofar as is
335   reasonably practicable, to fulfill the controller's obligation to respond to
336   consumer rights requests, (2) taking into account the nature of
337   processing and the information available to the processor, by assisting
338   the controller in meeting the controller's obligations in relation to the
339   security of processing the personal data and in relation to the

340 notification of a breach of security of the system of the processor, in
341 order to meet the controller's obligations, and (3) providing necessary
342 information to enable the controller to conduct and document data
343 protection assessments.

344   (b) A contract between a controller and a processor shall govern the
345 processor's data processing procedures with respect to processing
346 performed on behalf of the controller. The contract shall be binding and
347 clearly set forth instructions for processing data, the nature and purpose
348 of processing, the type of data subject to processing, the duration of
349 processing and the rights and obligations of both parties. The contract
350 shall also include requirements that the processor shall: (1) Ensure that
351 each person processing personal data is subject to a duty of
352 confidentiality with respect to the data, (2) at the controller's direction,
353 delete or return all personal data to the controller as requested at the
354 end of the provision of services, unless retention of the personal data is
355 required by law, (3) upon the reasonable request of the controller, make
356 available to the controller all information in its possession necessary to
357 demonstrate the processor's compliance with the obligations in sections
358 1 to 11, inclusive, of this act, (4) engage any subcontractor pursuant to a
359 written contract that requires the subcontractor to meet the obligations
360 of the processor with respect to the personal data, and (5) allow, and
361 cooperate with, reasonable assessments by the controller or the
362 controller's designated assessor, or the processor may arrange for a
363 qualified and independent assessor to conduct an assessment of the
364 processor's policies and technical and organizational measures in
365 support of the obligations under sections 1 to 11, inclusive, of this act,
366 using an appropriate and accepted control standard or framework and
367 assessment procedure for such assessments. The processor shall provide
368 a report of such assessment to the controller upon request.

369   (c) Nothing in this section shall be construed to relieve a controller or
370 a processor from the liabilities imposed on it by virtue of its role in the
371 processing relationship as defined in sections 1 to 11, inclusive, of this
372 act.

373   (d) Determining whether a person is acting as a controller or
374   processor with respect to a specific processing of data is a fact-based
375   determination that depends upon the context in which personal data is
376   to be processed. A processor that continues to adhere to a controller's
377   instructions with respect to a specific processing of personal data
378   remains a processor.

379   Sec. 7. (NEW) (*Effective January 1, 2023*) (a) A controller shall conduct
380   and document a data protection assessment of each of the following
381   processing activities involving personal data: (1) The processing of
382   personal data for purposes of targeted advertising, (2) the sale of
383   personal data, (3) the processing of personal data for purposes of
384   profiling, where such profiling presents a reasonably foreseeable risk of
385   (A) unfair or deceptive treatment of, or unlawful disparate impact on,
386   consumers, (B) financial, physical or reputational injury to consumers,
387   (C) a physical or other intrusion upon the solitude or seclusion, or the
388   private affairs or concerns, of consumers, where such intrusion would
389   be offensive to a reasonable person, or (D) other substantial injury to
390   consumers, (4) the processing of sensitive data, and (5) any processing
391   activities involving personal data that present a heightened risk of harm
392   to consumers.

393   (b) Data protection assessments conducted pursuant to subsection (a)
394   of this section shall identify and weigh the benefits that may flow,
395   directly and indirectly, from the processing to the controller, the
396   consumer, other stakeholders and the public against the potential risks
397   to the rights of the consumer associated with such processing, as
398   mitigated by safeguards that can be employed by the controller to
399   reduce such risks. The use of de-identified data and the reasonable
400   expectations of consumers, as well as the context of the processing and
401   the relationship between the controller and the consumer whose
402   personal data will be processed, shall be factored into this assessment
403   by the controller.

404   (c) The Attorney General may require that a controller disclose any
405   data protection assessment that is relevant to an investigation

406 conducted by the Attorney General, and the controller shall make the
407 data protection assessment available to the Attorney General. The
408 Attorney General may evaluate the data protection assessment for
409 compliance with the responsibilities set forth in sections 1 to 11,
410 inclusive, of this act. Data protection assessments shall be confidential
411 and shall be exempt from disclosure under the Freedom of Information
412 Act, as defined in section 1-200 of the general statutes. The disclosure of
413 a data protection assessment pursuant to a request from the Attorney
414 General shall not constitute a waiver of attorney-client privilege or work
415 product protection with respect to the assessment and any information
416 contained in the assessment.

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

419 (e) Data protection assessments conducted by a controller for the
420 purpose of compliance with other laws or regulations may comply
421 under this section if the assessments have a reasonably comparable
422 scope and effect.

423 (f) Data protection assessment requirements shall apply to processing
424 activities created or generated after January 1, 2023, and are not
425 retroactive.

426 Sec. 8. (NEW) (*Effective January 1, 2023*) (a) Any controller in
427 possession of de-identified data shall: (1) Take reasonable measures to
428 ensure that the data cannot be associated with a natural person, (2)
429 publicly commit to maintaining and using de-identified data without
430 attempting to re-identify the data, and (3) contractually obligate any
431 recipients of the de-identified data to comply with all provisions of
432 sections 1 to 11, inclusive, of this act.

433 (b) Nothing in sections 1 to 11, inclusive, of this act shall be construed
434 to (1) require a controller or processor to re-identify de-identified data
435 or pseudonymous data, or (2) maintain data in identifiable form, or
436 collect, obtain, retain or access any data or technology, in order to be

437 capable of associating an authenticated consumer request with personal
438 data.

439   (c) Nothing in sections 1 to 11, inclusive, of this act shall be construed
440 to require a controller or processor to comply with an authenticated
441 consumer rights request, if all of the following are true, if the controller:
442 (1) Is not reasonably capable of associating the request with the personal
443 data or it would be unreasonably burdensome for the controller to
444 associate the request with the personal data, (2) does not use the
445 personal data to recognize or respond to the specific consumer who is
446 the subject of the personal data, or associate the personal data with other
447 personal data about the same specific consumer, and (3) does not sell
448 the personal data to any third party or otherwise voluntarily disclose
449 the personal data to any third party other than a processor, except as
450 otherwise permitted in this section.

451   (d) Consumer rights shall not apply to pseudonymous data in cases
452 where the controller is able to demonstrate any information necessary
453 to identify the consumer is kept separately and is subject to effective
454 technical and organizational controls that prevent the controller from
455 accessing such information.

456   (e) A controller that discloses pseudonymous data or de-identified
457 data shall exercise reasonable oversight to monitor compliance with any
458 contractual commitments to which the pseudonymous data or de-
459 identified data is subject and shall take appropriate steps to address any
460 breaches of those contractual commitments.

461   Sec. 9. (NEW) (*Effective January 1, 2023*) (a) Nothing in sections 1 to 11,
462 inclusive, of this act shall be construed to restrict a controller's or
463 processor's ability to: (1) Comply with federal, state or municipal
464 ordinances or regulations, (2) comply with a civil, criminal or regulatory
465 inquiry, investigation, subpoena or summons by federal, state,
466 municipal or other governmental authorities, (3) cooperate with law-
467 enforcement agencies concerning conduct or activity that the controller
468 or processor reasonably and in good faith believes may violate federal,

469   state or municipal ordinances or regulations, (4) investigate, establish,
470   exercise, prepare for or defend legal claims, (5) provide a product or
471   service specifically requested by a consumer, (6) perform a contract to
472   which a consumer is a party, including fulfilling the terms of a written
473   warranty, (7) take steps at the request of a consumer prior to entering
474   into a contract, (8) take immediate steps to protect an interest that is
475   essential for the life or physical safety of the consumer or of another
476   natural person, and where the processing cannot be manifestly based on
477   another legal basis, (9) prevent, detect, protect against or respond to
478   security incidents, identity theft, fraud, harassment, malicious or
479   deceptive activities or any illegal activity, preserve the integrity or
480   security of systems or investigate, report or prosecute those responsible
481   for any such action, (10) engage in public or peer-reviewed scientific or
482   statistical research in the public interest that adheres to all other
483   applicable ethics and privacy laws and is approved, monitored and
484   governed by an institutional review board, or similar independent
485   oversight entities that determine (A) if the deletion of the information is
486   likely to provide substantial benefits that do not exclusively accrue to
487   the controller, (B) the expected benefits of the research outweigh the
488   privacy risks, and (C) if the controller has implemented reasonable
489   safeguards to mitigate privacy risks associated with research, including
490   any risks associated with re-identification, or (11) assist another
491   controller, processor, or third party with any of the obligations under
492   sections 1 to 11, inclusive, of this act.

493   (b) The obligations imposed on controllers or processors under
494   sections 1 to 11, inclusive, of this act shall not restrict a controller's or
495   processor's ability to collect, use, or retain data to: (1) Conduct internal
496   research to develop, improve, or repair products, services, or
497   technology, (2) effectuate a product recall, (3) identify and repair
498   technical errors that impair existing or intended functionality, or (4)
499   perform internal operations that are reasonably aligned with the
500   expectations of the consumer or reasonably anticipated based on the
501   consumer's existing relationship with the controller or are otherwise
502   compatible with processing data in furtherance of the provision of a

503 product or service specifically requested by a consumer or the
504 performance of a contract to which the consumer is a party.

505 (c) The obligations imposed on controllers or processors under
506 sections 1 to 11, inclusive, of this act shall not apply where compliance
507 by the controller or processor with said sections would violate an
508 evidentiary privilege under the laws of this state. Nothing in sections 1
509 to 11, inclusive, of this act shall be construed to prevent a controller or
510 processor from providing personal data concerning a consumer to a
511 person covered by an evidentiary privilege under the laws of the state
512 as part of a privileged communication.

513 (d) A controller or processor that discloses personal data to a third-
514 party controller or processor, in compliance with the requirements of
515 sections 1 to 11, inclusive, of this act, is not in violation of said sections
516 if the third-party controller or processor that receives and processes
517 such personal data is in violation of said sections, provided, at the time
518 of disclosing the personal data, the disclosing controller or processor did
519 not have actual knowledge that the recipient intended to commit a
520 violation of said sections. A third-party controller or processor receiving
521 personal data from a controller or processor in compliance with the
522 requirements of sections 1 to 11, inclusive, of this act is likewise not in
523 violation of said sections for the transgressions of the controller or
524 processor from which it receives such personal data.

525 (e) Nothing in sections 1 to 11, inclusive, of this act shall be construed
526 as an obligation imposed on controllers and processors that adversely
527 affects the rights or freedoms of any persons, such as exercising the right
528 of free speech pursuant to the First Amendment to the United States
529 Constitution, or applies to the processing of personal data by a person
530 in the course of a purely personal or household activity.

531 (f) Personal data processed by a controller pursuant to sections 1 to
532 11, inclusive, of this act shall not be processed for any purpose other
533 than those expressly listed in this section unless otherwise allowed by
534 sections 1 to 11, inclusive, of this act. Personal data processed by a

535   controller pursuant to this section may be processed to the extent that
536   such processing is: (1) Reasonably necessary and proportionate to the
537   purposes listed in this section, and (2) adequate, relevant and limited to
538   what is necessary in relation to the specific purposes listed in this
539   section. Personal data collected, used, or retained pursuant to subsection
540   (b) of this section shall, where applicable, take into account the nature
541   and purpose or purposes of such collection, use, or retention. Such data
542   shall be subject to reasonable administrative, technical, and physical
543   measures to protect the confidentiality, integrity, and accessibility of the
544   personal data and to reduce reasonably foreseeable risks of harm to
545   consumers relating to such collection, use, or retention of personal data.

546   (g) If a controller processes personal data pursuant to an exemption
547   in this section, the controller bears the burden of demonstrating that
548   such processing qualifies for the exemption and complies with the
549   requirements in subsection (f) of this section.

550   (h) Processing personal data for the purposes expressly identified in
551   this section shall not solely make an entity a controller with respect to
552   such processing.

553   Sec. 10. (NEW) (*Effective January 1, 2023*) (a) The Attorney General
554   shall have exclusive authority to enforce violations of sections 1 to 11,
555   inclusive, of this act.

556   (b) Prior to initiating any action under sections 1 to 11, inclusive, of
557   this act, the Attorney General shall provide a controller or processor not
558   less than thirty days' written notice identifying the specific provisions
559   of said sections the Attorney General, on behalf of a consumer, alleges
560   have been or are being violated. If, prior to the expiration of such time
561   period, the controller or processor cures the noticed violation and
562   provides the Attorney General an express written statement that the
563   alleged violations have been cured and that no further violations shall
564   occur, no action for statutory damages shall be initiated against the
565   controller or processor.

566	(c) If a controller or processor continues to violate sections 1 to 11,
567	inclusive, of this act in breach of an express written statement provided
568	to the consumer under this section, the Attorney General may initiate a
569	civil action in Superior Court and seek damages not exceeding seven
570	thousand five hundred dollars for each violation of sections 1 to 11,
571	inclusive, of this act.

572	(d) Nothing in sections 1 to 11, inclusive, of this act shall be construed
573	as providing the basis for, or be subject to, a private right of action for
574	violations of said sections or any other law.

575	Sec. 11. (NEW) (*Effective January 1, 2023*) (a) The Attorney General
576	shall have exclusive authority to enforce sections 1 to 10, inclusive, of
577	this act by bringing an action in the name of the state, or on behalf of
578	persons residing in this state.

579	(b) Any controller or processor that violates sections 1 to 10, inclusive,
580	of this act shall be liable for a civil penalty of not more than seven
581	thousand five hundred dollars for each violation.

582	(c) The Attorney General may recover reasonable expenses incurred
583	in investigating and preparing the case, including attorney fees, of any
584	action initiated under sections 1 to 10, inclusive, of this act.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*January 1, 2023*	New section
Sec. 2	*January 1, 2023*	New section
Sec. 3	*January 1, 2023*	New section
Sec. 4	*January 1, 2023*	New section
Sec. 5	*January 1, 2023*	New section
Sec. 6	*January 1, 2023*	New section
Sec. 7	*January 1, 2023*	New section
Sec. 8	*January 1, 2023*	New section
Sec. 9	*January 1, 2023*	New section
Sec. 10	*January 1, 2023*	New section
Sec. 11	*January 1, 2023*	New section

GL   *Joint Favorable Subst.*

JUD   *Joint Favorable*

APP   *Joint Favorable*