

Senator Kirk A. Cullimore proposes the following substitute bill:

CONSUMER PRIVACY ACT

2022 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Kirk A. Cullimore

House Sponsor: Brady Brammer

LONG TITLE

General Description:

This bill enacts the Utah Consumer Privacy Act.

Highlighted Provisions:

This bill:

- ▶ defines terms;
- ▶ provides consumers the right to:
 - access and delete certain personal data maintained by certain businesses; and
 - opt out of the collection and use of personal data for certain purposes;
- ▶ requires certain businesses that control and process consumers' personal data to:
 - safeguard consumers' personal data;
 - provide clear information to consumers regarding how the consumers' personal data are used; and
 - accept and comply with a consumer's request to exercise the consumer's rights under this bill;
- ▶ creates a right for a consumer to know what personal data a business collects, how the business uses the personal data, and whether the business sells the personal data;
- ▶ upon request and subject to exceptions, requires a business to delete a consumer's personal data or stop selling the consumer's personal data;



26 ▶ allows the Division of Consumer Protection to accept and investigate consumer
27 complaints regarding the processing of personal data;

28 ▶ authorizes the Office of the Attorney General to take enforcement action and
29 impose penalties; and

30 ▶ makes technical changes.

31 **Money Appropriated in this Bill:**

32 None

33 **Other Special Clauses:**

34 This bill provides a special effective date.

35 **Utah Code Sections Affected:**

36 AMENDS:

37 **13-2-1**, as last amended by Laws of Utah 2021, Chapter 266

38 ENACTS:

39 **13-61-101**, Utah Code Annotated 1953

40 **13-61-102**, Utah Code Annotated 1953

41 **13-61-103**, Utah Code Annotated 1953

42 **13-61-201**, Utah Code Annotated 1953

43 **13-61-202**, Utah Code Annotated 1953

44 **13-61-203**, Utah Code Annotated 1953

45 **13-61-301**, Utah Code Annotated 1953

46 **13-61-302**, Utah Code Annotated 1953

47 **13-61-303**, Utah Code Annotated 1953

48 **13-61-304**, Utah Code Annotated 1953

49 **13-61-305**, Utah Code Annotated 1953

50 **13-61-401**, Utah Code Annotated 1953

51 **13-61-402**, Utah Code Annotated 1953

52 **13-61-403**, Utah Code Annotated 1953

53 **13-61-404**, Utah Code Annotated 1953

54

55 *Be it enacted by the Legislature of the state of Utah:*

56 Section 1. Section **13-2-1** is amended to read:

57 **13-2-1. Consumer protection division established -- Functions.**

58 (1) There is established within the Department of Commerce the Division of Consumer
59 Protection.

60 (2) The division shall administer and enforce the following:

61 (a) Chapter 5, Unfair Practices Act;

62 (b) Chapter 10a, Music Licensing Practices Act;

63 (c) Chapter 11, Utah Consumer Sales Practices Act;

64 (d) Chapter 15, Business Opportunity Disclosure Act;

65 (e) Chapter 20, New Motor Vehicle Warranties Act;

66 (f) Chapter 21, Credit Services Organizations Act;

67 (g) Chapter 22, Charitable Solicitations Act;

68 (h) Chapter 23, Health Spa Services Protection Act;

69 (i) Chapter 25a, Telephone and Facsimile Solicitation Act;

70 (j) Chapter 26, Telephone Fraud Prevention Act;

71 (k) Chapter 28, Prize Notices Regulation Act;

72 (l) Chapter 32a, Pawnshop and Secondhand Merchandise Transaction Information Act;

73 (m) Chapter 34, Utah Postsecondary Proprietary School Act;

74 (n) Chapter 34a, Utah Postsecondary School State Authorization Act;

75 (o) Chapter 41, Price Controls During Emergencies Act;

76 (p) Chapter 42, Uniform Debt-Management Services Act;

77 (q) Chapter 49, Immigration Consultants Registration Act;

78 (r) Chapter 51, Transportation Network Company Registration Act;

79 (s) Chapter 52, Residential Solar Energy Disclosure Act;

80 (t) Chapter 53, Residential, Vocational and Life Skills Program Act;

81 (u) Chapter 54, Ticket Website Sales Act;

82 (v) Chapter 56, Ticket Transferability Act; [~~and~~]

83 (w) Chapter 57, Maintenance Funding Practices Act[~~;~~]; and

84 (x) Chapter 61, Utah Consumer Privacy Act.

85 Section 2. Section **13-61-101** is enacted to read:

86 **CHAPTER 61. UTAH CONSUMER PRIVACY ACT**

87 **Part 1. General Provisions**

88 13-61-101. Definitions.

89 As used in this chapter:

90 (1) "Account" means the Consumer Privacy Restricted Account established in Section
91 13-61-403.

92 (2) "Affiliate" means an entity that:

93 (a) controls, is controlled by, or is under common control with another entity; or

94 (b) shares common branding with another entity.

95 (3) "Aggregated data" means information that relates to a group or category of
96 consumers:

97 (a) from which individual consumer identities have been removed; and

98 (b) that is not linked or reasonably linkable to any consumer.

99 (4) "Air carrier" means the same as that term is defined in 49 U.S.C. Sec. 40102.

100 (5) "Authenticate" means to use reasonable means to determine that a consumer's
101 request to exercise the rights described in Section 13-61-201 is made by the consumer who is
102 entitled to exercise those rights.

103 (6) (a) "Biometric data" means data generated by automatic measurements of an
104 individual's unique biological characteristics.

105 (b) "Biometric data" includes data described in Subsection (6)(a) that are ~~or~~ [:

106 ~~(i)~~ ~~←~~ generated by automatic measurements of an individual's fingerprint, voiceprint, eye
107 retinas, irises, or any other unique biological pattern or characteristic that is used to identify a
108 specific individual ~~or~~ ~~;~~ . ~~←~~

109 ~~←~~ [(ii) captured from a patient in a health care setting.] ~~←~~

110 (c) "Biometric data" does not include:

111 (i) a physical or digital photograph;

112 (ii) a video or audio recording;

113 (iii) data generated from an item described in Subsection (6)(c)(i) or (ii); ~~or~~ [

113a (iv) information captured from a patient in a health care setting; or ~~←~~

114 ~~←~~ [(iv)] (v) ~~←~~ information collected, used, or stored for treatment, payment, or health
114a care

115 operations as those terms are defined in 45 C.F.R. Parts 160, 162, and 164.

116 (7) "Business associate" means the same as that term is defined in 45 C.F.R. Sec.
117 160.103.

118 (8) "Child" means an individual younger than 13 years old.

119 (9) "Consent" means an affirmative act by a consumer that unambiguously indicates
120 the consumer's voluntary and informed agreement to allow a person to process personal data
121 related to the consumer.

122 (10) (a) "Consumer" means an individual who is a resident of the state acting in an
123 individual or household context.

124 (b) "Consumer" does not include an individual acting in an employment or commercial
125 context.

126 (11) "Control" or "controlled" as used in Subsection (2) means:

127 (a) ownership of, or the power to vote, more than 50% of the outstanding shares of any
128 class of voting securities of an entity;

129 (b) control in any manner over the election of a majority of the directors or of the
130 individuals exercising similar functions; or

131 (c) the power to exercise controlling influence of the management of an entity.

132 (12) "Controller" means a person doing business in the state who determines the
133 purposes for which and the means by which personal data is processed, regardless of whether
134 the person makes the determination alone or with others.

135 (13) "Covered entity" means the same as that term is defined in 45 C.F.R. Sec.
136 160.103.

137 (14) "Deidentified data" means data that:

138 (a) cannot reasonably be linked to an identified individual or an identifiable individual;
139 and

140 (b) are possessed by a controller who:

141 (i) takes reasonable measures to ensure that a person cannot associate the data with an
142 individual;

143 (ii) publicly commits to maintain and use the data only in deidentified form and not
144 attempt to reidentify the data; and

145 (iii) contractually obligates any recipients of the data to comply with the requirements
146 described in Subsections (14)(b)(i) and (ii).

147 (15) "Director" means the director of the Division of Consumer Protection.

148 (16) "Division" means the Division of Consumer Protection created in Section [13-2-1](#).

149 (17) "Governmental entity" means the same as that term is defined in Section

150 [63G-2-103.](#)

151 (18) "Health care facility" means the same as that term is defined in Section [26-21-2](#).

152 (19) "Health care provider" means the same as that term is defined in Section [26-21-2](#).

153 (20) "Identifiable individual" means an individual who can be readily identified,

154 directly or indirectly.

155 (21) "Institution of higher education" means a public or private institution of higher
156 education.

157 (22) "Local political subdivision" means the same as that term is defined in Section

158 [11-14-102.](#)

159 (23) "Nonprofit corporation" means:

160 (a) the same as that term is defined in Section [16-6a-102](#); or

161 (b) a foreign nonprofit corporation as defined in Section [16-6a-102](#).

162 (24) (a) "Personal data" means information that is linked or reasonably linkable to an
163 identified individual or an identifiable individual.

164 (b) "Personal data" does not include deidentified data, aggregated data, or publicly
165 available information.

166 (25) "Process" means an operation or set of operations performed on personal data,
167 including collection, use, storage, disclosure, analysis, deletion, or modification of personal
168 data.

169 (26) "Processor" means a person who processes personal data on behalf of a controller.

170 (27) "Protected health information" means the same as that term is defined in 45 C.F.R.
171 Sec. 160.103.

172 (28) "Pseudonymous data" means personal data that cannot be attributed to a specific
173 individual without the use of additional information, if the additional information is:

174 (a) kept separate from the consumer's personal data; and

175 (b) subject to appropriate technical and organizational measures to ensure that the
176 personal data are not attributable to an identified individual or an identifiable individual.

177 (29) "Publicly available information" means information that a person:

178 (a) lawfully obtains from a record of a governmental entity;

179 (b) reasonably believes a consumer or widely distributed media has lawfully made
180 available to the general public; or

181 (c) if the consumer has not restricted the information to a specific audience, obtains
182 from a person to whom the consumer disclosed the information.

183 (30) "Right" means a consumer right described in Section 13-61-201.

184 (31) (a) "Sale," "sell," or "sold" means the exchange of personal data for monetary
185 consideration by a controller to a third party.

186 (b) "Sale," "sell," or "sold" does not include:

187 (i) a controller's disclosure of personal data to a processor who processes the personal
188 data on behalf of the controller;

189 (ii) a controller's disclosure of personal data to an affiliate of the controller;

190 (iii) considering the context in which the consumer provided the personal data to the
191 controller, a controller's disclosure of personal data to a third party if the purpose is consistent
192 with a consumer's reasonable expectations;

193 (iv) the disclosure or transfer of personal data when a consumer directs a controller to:

194 (A) disclose the personal data; or

195 (B) interact with one or more third parties;

196 (v) a consumer's disclosure of personal data to a third party for the purpose of
197 providing a product or service requested by the consumer or a parent or legal guardian of a
198 child;

199 (vi) the disclosure of information that the consumer:

200 (A) intentionally makes available to the general public via a channel of mass media;

201 and

202 (B) does not restrict to a specific audience; or

203 (vii) a controller's transfer of personal data to a third party as an asset that is part of a
204 proposed or actual merger, an acquisition, or a bankruptcy in which the third party assumes
205 control of all or part of the controller's assets.

206 (32) (a) "Sensitive data" means:

207 (i) personal data that reveals:

208 (A) an individual's racial or ethnic origin;

209 (B) an individual's religious beliefs;

210 (C) an individual's sexual orientation;

211 (D) an individual's citizenship or immigration status; or

212 (E) information regarding an individual's medical history, mental or physical health
213 condition, or medical treatment or diagnosis by a health care professional;
214 (ii) the processing of genetic personal data or biometric data, if the processing is for the
215 purpose of identifying a specific individual; or
216 (iii) specific geolocation data.
217 (b) "Sensitive data" does not include personal data that reveals an individual's:
218 (i) racial or ethnic origin, if the personal data is processed by a video communication
219 service; or
220 (ii) if the personal data is processed by a person licensed to provide health care under
221 Title 26, Chapter 21, Health Care Facility Licensing and Inspection Act, or Title 58,
222 Occupations and Professions, information regarding an individual's medical history, mental or
223 physical health condition, or medical treatment or diagnosis by a health care professional.
224 (33) (a) "Specific geolocation data" means information derived from technology,
225 including global position system level latitude and longitude coordinates, that directly
226 identifies an individual's specific location, accurate within a radius of 1,750 feet or less.
227 (b) "Specific geolocation data" does not include:
228 (i) the content of a communication; or
229 (ii) any data generated by or connected to advanced utility metering infrastructure
230 systems or equipment for use by a utility.
231 (34) (a) "Targeted advertising" means displaying an advertisement to a consumer
232 where the advertisement is selected based on personal data obtained from the consumer's
233 activities over time and across nonaffiliated websites or online applications to predict the
234 consumer's preferences or interests.
235 (b) "Targeted advertising" does not include advertising:
236 (i) based on a consumer's activities within a controller's website or online application
237 or any affiliated website or online application;
238 (ii) based on the context of a consumer's current search query or visit to a website or
239 online application;
240 (iii) directed to a consumer in response to the consumer's request for information,
241 product, a service, or feedback; or
242 (iv) processing personal data solely to measure or report advertising;

243 (A) performance;

244 (B) reach; or

245 (C) frequency.

246 (35) "Third party" means a person other than:

247 (a) the consumer, controller, or processor; or

248 (b) an affiliate or contractor of the controller or the processor.

249 (36) "Trade secret" means information, including a formula, pattern, compilation,
250 program, device, method, technique, or process, that:

251 (a) derives independent economic value, actual or potential, from not being generally
252 known to, and not being readily ascertainable by proper means by, other persons who can
253 obtain economic value from the information's disclosure or use; and

254 (b) is the subject of efforts that are reasonable under the circumstances to maintain the
255 information's secrecy.

256 Section 3. Section **13-61-102** is enacted to read:

257 **13-61-102. Applicability.**

258 (1) This chapter applies to any controller or processor who:

259 (a) (i) conducts business in the state; or

260 (ii) produces a product or service that is targeted to consumers who are residents of the
261 state;

262 (b) has annual revenue of \$25,000,000 or more; and

263 (c) satisfies one or more of the following thresholds:

264 (i) during a calendar year, controls or processes personal data of 100,000 or more
265 consumers; or

266 (ii) derives over 50% of the entity's gross revenue from the sale of personal data and
267 controls or processes personal data of 25,000 or more consumers.

268 (2) This chapter does not apply to:

269 (a) a governmental entity or a third party under contract with a governmental entity
270 when the third party is acting on behalf of the governmental entity;

271 (b) a tribe;

272 (c) an institution of higher education;

273 (d) a nonprofit corporation;

- 274 (e) a covered entity;
- 275 (f) a business associate;
- 276 (g) information that meets the definition of:
- 277 (i) protected health information for purposes of the federal Health Insurance Portability
- 278 and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., and related regulations;
- 279 (ii) patient identifying information for purposes of 42 C.F.R. Part 2;
- 280 (iii) identifiable private information for purposes of the Federal Policy for the
- 281 Protection of Human Subjects, 45 C.F.R. Part 46;
- 282 (iv) identifiable private information or personal data collected as part of human
- 283 subjects research pursuant to or under the same standards as:
- 284 (A) the good clinical practice guidelines issued by the International Council for
- 285 Harmonisation; or
- 286 (B) the Protection of Human Subjects under 21 C.F.R. Part 50 and Institutional Review
- 287 Boards under 21 C.F.R. Part 56;
- 288 (v) personal data used or shared in research conducted in accordance with one or more
- 289 of the requirements described in Subsection (2)(g)(iv);
- 290 (vi) information and documents created specifically for, and collected and maintained
- 291 by, a committee listed in Section [26-1-7](#);
- 292 (vii) information and documents created for purposes of the federal Health Care
- 293 Quality Improvement Act of 1986, 42 U.S.C. Sec. 11101 et seq., and related regulations;
- 294 (viii) patient safety work product for purposes of 42 C.F.R. Part 3; or
- 295 (ix) information that is:
- 296 (A) deidentified in accordance with the requirements for deidentification set forth in 45
- 297 C.F.R. Part 164; and
- 298 (B) derived from any of the health care-related information listed in this Subsection
- 299 (2)(g);
- 300 (h) information originating from, and intermingled to be indistinguishable with,
- 301 information under Subsection (2)(g) that is maintained by:
- 302 (i) a health care facility or health care provider; or
- 303 (ii) a program or a qualified service organization as defined in 42 C.F.R. Sec. 2.11;
- 304 (i) information used only for public health activities and purposes as described in 45

305 C.F.R. Sec. 164.512;
306 (j) (i) an activity by:
307 (A) a consumer reporting agency, as defined in 15 U.S.C. Sec. 1681a;
308 (B) a furnisher of information, as set forth in 15 U.S.C. Sec. 1681s-2, who provides
309 information for use in a consumer report, as defined in 15 U.S.C. Sec. 1681a; or
310 (C) a user of a consumer report, as set forth in 15 U.S.C. Sec. 1681b;
311 (ii) subject to regulation under the federal Fair Credit Reporting Act, 15 U.S.C. Sec.
312 1681 et seq.; and
313 (iii) involving the collection, maintenance, disclosure, sale, communication, or use of
314 any personal data bearing on a consumer's:
315 (A) credit worthiness;
316 (B) credit standing;
317 (C) credit capacity;
318 (D) character;
319 (E) general reputation;
320 (F) personal characteristics; or
321 (G) mode of living;
322 (k) a financial institution or an affiliate of a financial institution governed by, or
323 personal data collected, processed, sold, or disclosed in accordance with, Title V of the
324 Gramm-Leach-Bliley Act, 15 U.S.C. Sec. 6801 et seq., and related regulations;
325 (l) personal data collected, processed, sold, or disclosed in accordance with the federal
326 Driver's Privacy Protection Act of 1994, 18 U.S.C. Sec. 2721 et seq.;
327 (m) personal data regulated by the federal Family Education Rights and Privacy Act,
328 20 U.S.C. Sec. 1232g, and related regulations;
329 (n) personal data collected, processed, sold, or disclosed in accordance with the federal
330 Farm Credit Act of 1971, 12 U.S.C. Sec. 2001 et seq.;
331 (o) data that are processed or maintained:
332 (i) in the course of an individual applying to, being employed by, or acting as an agent
333 or independent contractor of a controller, processor, or third party, to the extent the collection
334 and use of the data are related to the individual's role;
335 (ii) as the emergency contact information of an individual described in Subsection

336 (2)(o)(i) and used for emergency contact purposes; or
337 (iii) to administer benefits for another individual relating to an individual described in
338 Subsection (2)(o)(i) and used for the purpose of administering the benefits;

339 (p) an individual's processing of personal data for purely personal or household
340 purposes; or

341 (q) an air carrier.

342 (3) A controller is in compliance with any obligation to obtain parental consent under
343 this chapter if the controller complies with the verifiable parental consent mechanisms under
344 the Children's Online Privacy Protection Act, 15 U.S.C. Sec. 6501 et seq., and the act's
345 implementing regulations and exemptions.

346 (4) This chapter does not require a person to take any action in conflict with the federal
347 Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. Sec. 1320d et seq., or
348 related regulations.

349 Section 4. Section **13-61-103** is enacted to read:

350 **13-61-103. Preemption -- Reference to other laws.**

351 (1) This chapter supersedes and preempts any ordinance, resolution, rule, or other
352 regulation adopted by a local political subdivision regarding the processing of personal data by
353 a controller or processor.

354 (2) Any reference to federal law in this chapter includes any rules or regulations
355 promulgated under the federal law.

356 Section 5. Section **13-61-201** is enacted to read:

357 **Part 2. Rights Relating to Personal Data**

358 **13-61-201. Consumer rights -- Access -- Deletion -- Portability -- Opt out of**
359 **certain processing.**

360 (1) A consumer has the right to:

361 (a) confirm whether a controller is processing the consumer's personal data; and

362 (b) access the consumer's personal data.

363 (2) A consumer has the right to delete the consumer's personal data that the consumer
364 provided to the controller.

365 (3) A consumer has the right to obtain a copy of the consumer's personal data, that the
366 consumer previously provided to the controller, in a format that:

367 (a) to the extent technically feasible, is portable;
368 (b) to the extent practicable, is readily usable; and
369 (c) allows the consumer to transmit the data to another controller without impediment,
370 where the processing is carried out by automated means.

371 (4) A consumer has the right to opt out of the processing of the consumer's personal
372 data for purposes of:

373 (a) targeted advertising; or
374 (b) the sale of personal data.

375 (5) Nothing in this section requires a person to cause a breach of security system as
376 defined in Section [13-44-102](#).

377 Section 6. Section **13-61-202** is enacted to read:

378 **13-61-202. Exercising consumer rights.**

379 (1) A consumer may exercise a right by submitting a request to a controller, by means
380 prescribed by the controller, specifying the right the consumer intends to exercise.

381 (2) In the case of processing personal data concerning a known child, the parent or
382 legal guardian of the known child shall exercise a right on the child's behalf.

383 (3) In the case of processing personal data concerning a consumer subject to
384 guardianship, conservatorship, or other protective arrangement under Title 75, Chapter 5,
385 Protection of Persons Under Disability and Their Property, the guardian or the conservator of
386 the consumer shall exercise a right on the consumer's behalf.

387 Section 7. Section **13-61-203** is enacted to read:

388 **13-61-203. Controller's response to requests.**

389 (1) Subject to the other provisions of this chapter, a controller shall comply with a
390 consumer's request under Section [13-61-202](#) to exercise a right.

391 (2) (a) Within 45 days after the day on which a controller receives a request to exercise
392 a right, the controller shall:

393 (i) take action on the consumer's request; and
394 (ii) inform the consumer of any action taken on the consumer's request.

395 (b) The controller may extend once the initial 45-day period by an additional 45 days if
396 reasonably necessary due to the complexity of the request or the volume of the requests
397 received by the controller.

398 (c) If a controller extends the initial 45-day period, before the initial 45-day period
399 expires, the controller shall:

400 (i) inform the consumer of the extension, including the length of the extension; and

401 (ii) provide the reasons the extension is reasonably necessary as described in

402 Subsection (2)(b).

403 (d) The 45-day period does not apply if the controller reasonably suspects the
404 consumer's request is fraudulent and the controller is not able to authenticate the request before
405 the 45-day period expires.

406 (3) If, in accordance with this section, a controller chooses not to take action on a
407 consumer's request, the controller shall within 45 days after the day on which the controller
408 receives the request, inform the consumer of the reasons for not taking action.

409 (4) (a) A controller may not charge a fee for information in response to a request,
410 unless the request is the consumer's second or subsequent request during the same 12-month
411 period.

412 (b) (i) Notwithstanding Subsection (4)(a), a controller may charge a reasonable fee to
413 cover the administrative costs of complying with a request or refuse to act on a request, if:

414 (A) the request is excessive, repetitive, technically infeasible, or manifestly unfounded;

415 (B) the controller reasonably believes the primary purpose in submitting the request
416 was something other than exercising a right; or

417 (C) the request, individually or as part of an organized effort, harasses, disrupts, or
418 imposes undue burden on the resources of the controller's business.

419 (ii) A controller that charges a fee or refuses to act in accordance with this Subsection
420 (4)(b) bears the burden of demonstrating the request satisfied one or more of the criteria
421 described in Subsection (4)(b)(i).

422 (5) If a controller is unable to authenticate a consumer request to exercise a right
423 described in Section [13-61-201](#) using commercially reasonable efforts, the controller:

424 (a) is not required to comply with the request; and

425 (b) may request that the consumer provide additional information reasonably necessary
426 to authenticate the request.

427 Section 8. Section **13-61-301** is enacted to read:

428 **Part 3. Requirements for Controllers and Processors**

429 **13-61-301. Responsibility according to role.**

430 (1) A processor shall:

431 (a) adhere to the controller's instructions; and

432 (b) taking into account the nature of the processing and information available to the
433 processor, by appropriate technical and organizational measures, insofar as reasonably
434 practicable, assist the controller in meeting the controller's obligations, including obligations
435 related to the security of processing personal data and notification of a breach of security
436 system described in Section [13-44-202](#).

437 (2) Before a processor performs processing on behalf of a controller, the processor and
438 controller shall enter into a contract that:

439 (a) clearly sets forth instructions for processing personal data, the nature and purpose
440 of the processing, the type of data subject to processing, the duration of the processing, and the
441 parties' rights and obligations;

442 (b) requires the processor to ensure each person processing personal data is subject to a
443 duty of confidentiality with respect to the personal data; and

444 (c) requires the processor to engage any subcontractor pursuant to a written contract
445 that requires the subcontractor to meet the same obligations as the processor with respect to the
446 personal data.

447 (3) (a) Determining whether a person is acting as a controller or processor with respect
448 to a specific processing of data is a fact-based determination that depends upon the context in
449 which personal data are to be processed.

450 (b) A processor that adheres to a controller's instructions with respect to a specific
451 processing of personal data remains a processor.

452 Section 9. Section **13-61-302** is enacted to read:

453 **13-61-302. Responsibilities of controllers -- Transparency -- Purpose specification**
454 **and data minimization -- Consent for secondary use -- Security -- Nondiscrimination --**
455 **Nonretaliation -- Nonwaiver of consumer rights.**

456 (1) (a) A controller shall provide consumers with a reasonably accessible and clear
457 privacy notice that includes:

458 (i) the categories of personal data processed by the controller;

459 (ii) the purposes for which the categories of personal data are processed;

460 (iii) how consumers may exercise a right;
461 (iv) the categories of personal data that the controller shares with third parties, if any;
462 and
463 (v) the categories of third parties, if any, with whom the controller shares personal data.
464 (b) If a controller sells a consumer's personal data to one or more third parties or
465 engages in targeted advertising, the controller shall clearly and conspicuously disclose to the
466 consumer the manner in which the consumer may exercise the right to opt out of the:
467 (i) sale of the consumer's personal data; or
468 (ii) processing for targeted advertising.
469 (2) (a) A controller shall establish, implement, and maintain reasonable administrative,
470 technical, and physical data security practices designed to:
471 (i) protect the confidentiality and integrity of personal data; and
472 (ii) reduce reasonably foreseeable risks of harm to consumers relating to the processing
473 of personal data.
474 (b) Considering the controller's business size, scope, and type, a controller shall use
475 data security practices that are appropriate for the volume and nature of the personal data at
476 issue.
477 (3) Except as otherwise provided in this chapter, a controller may not process sensitive
478 data collected from a consumer without:
479 (a) first presenting the consumer with clear notice and an opportunity to opt out of the
480 processing; or
481 (b) in the case of the processing of personal data concerning a known child, processing
482 the data in accordance with the federal Children's Online Privacy Protection Act, 15 U.S.C.
483 Sec. 6501 et seq., and the act's implementing regulations and exemptions.
484 (4) (a) A controller may not discriminate against a consumer for exercising a right by:
485 (i) denying a good or service to the consumer;
486 (ii) charging the consumer a different price or rate for a good or service; or
487 (iii) providing the consumer a different level of quality of a good or service.
488 (b) This Subsection (4) does not prohibit a controller from offering a different price,
489 rate, level, quality, or selection of a good or service to a consumer, including offering a good or
490 service for no fee or at a discount, if:

- 491 (i) the consumer has opted out of targeted advertising; or
- 492 (ii) the offer is related to the consumer's voluntary participation in a bona fide loyalty,
- 493 rewards, premium features, discounts, or club card program.

494 (5) A controller is not required to provide a product, service, or functionality to a
495 consumer if:

496 (a) the consumer's personal data are or the processing of the consumer's personal data
497 is reasonably necessary for the controller to provide the consumer the product, service, or
498 functionality; and

499 (b) the consumer does not:

- 500 (i) provide the consumer's personal data to the controller; or
- 501 (ii) allow the controller to process the consumer's personal data.

502 (6) Any provision of a contract that purports to waive or limit a consumer's right under
503 this chapter is void.

504 Section 10. Section **13-61-303** is enacted to read:

505 **13-61-303. Processing deidentified data or pseudonymous data.**

506 (1) The provisions of this chapter do not require a controller or processor to:

- 507 (a) reidentify deidentified data or pseudonymous data;
- 508 (b) maintain data in identifiable form or obtain, retain, or access any data or technology
509 for the purpose of allowing the controller or processor to associate a consumer request with
510 personal data; or

511 (c) comply with an authenticated consumer request to exercise a right described in
512 Subsections [13-61-202](#)(1) through (3), if:

513 (i) (A) the controller is not reasonably capable of associating the request with the
514 personal data; or

515 (B) it would be unreasonably burdensome for the controller to associate the request
516 with the personal data;

517 (ii) the controller does not:

518 (A) use the personal data to recognize or respond to the consumer who is the subject of
519 the personal data; or

520 (B) associate the personal data with other personal data about the consumer; and

521 (iii) the controller does not sell or otherwise disclose the personal data to any third

522 party other than a processor, except as otherwise permitted in this section.

523 (2) The rights described in Subsections 13-61-201(1) through (3) do not apply to
524 pseudonymous data if a controller demonstrates that any information necessary to identify a
525 consumer is kept:

526 (a) separately; and

527 (b) subject to appropriate technical and organizational measures to ensure the personal
528 data are not attributed to an identified individual or an identifiable individual.

529 (3) A controller who uses pseudonymous data or deidentified data shall take reasonable
530 steps to ensure the controller:

531 (a) complies with any contractual obligations to which the pseudonymous data or
532 deidentified data are subject; and

533 (b) promptly addresses any breach of a contractual obligation described in Subsection

534 (3)(a).

535 Section 11. Section **13-61-304** is enacted to read:

536 **13-61-304. Limitations.**

537 (1) The requirements described in this chapter do not restrict a controller or processor's
538 ability to:

539 (a) comply with a federal, state, or local law, rule, or regulation;

540 (b) comply with a civil, criminal, or regulatory inquiry, investigation, subpoena, or
541 summons by a federal, state, local, or other governmental entity;

542 (c) cooperate with a law enforcement agency concerning activity that the controller or
543 processor reasonably and in good faith believes may violate federal, state, or local laws, rules,
544 or regulations;

545 (d) investigate, establish, exercise, prepare for, or defend a legal claim;

546 (e) provide a product or service requested by a consumer or a parent or legal guardian
547 of a child;

548 (f) perform a contract to which the consumer or the parent or legal guardian of a child
549 is a party, including fulfilling the terms of a written warranty or taking steps at the request of
550 the consumer or parent or legal guardian before entering into the contract with the consumer;

551 (g) take immediate steps to protect an interest that is essential for the life or physical
552 safety of the consumer or of another individual;

553 (h) (i) detect, prevent, protect against, or respond to a security incident, identity theft,
554 fraud, harassment, malicious or deceptive activity, or any illegal activity; or

555 (ii) investigate, report, or prosecute a person responsible for an action described in
556 Subsection (1)(h)(i);

557 (i) (i) preserve the integrity or security of systems; or

558 (ii) investigate, report, or prosecute a person responsible for harming or threatening the
559 integrity or security of systems, as applicable;

560 (j) if the controller discloses the processing in a notice described in Section [13-61-302](#),
561 engage in public or peer-reviewed scientific, historical, or statistical research in the public
562 interest that adheres to all other applicable ethics and privacy laws;

563 (k) assist another person with an obligation described in this subsection;

564 (l) process personal data to:

565 (i) conduct internal analytics or other research to develop, improve, or repair a
566 controller or processor's product, service, or technology;

567 (ii) identify and repair technical errors that impair existing or intended functionality; or

568 (iii) effectuate a product recall;

569 (m) process personal data to perform an internal operation that is:

570 (i) reasonably aligned with the consumer's expectations based on the consumer's
571 existing relationship with the controller; or

572 (ii) otherwise compatible with processing to aid the controller or processor in
573 providing a product or service specifically requested by a consumer or a parent or legal
574 guardian of a child or the performance of a contract to which the consumer or a parent or legal
575 guardian of a child is a party; or

576 (n) retain a consumer's email address to comply with the consumer's request to exercise
577 a right.

578 (2) This chapter does not apply if a controller or processor's compliance with this
579 chapter:

580 (a) violates an evidentiary privilege under Utah law;

581 (b) as part of a privileged communication, prevents a controller or processor from
582 providing personal data concerning a consumer to a person covered by an evidentiary privilege
583 under Utah law; or

- 584 (c) adversely affect the privacy or other rights of any person.
585 (3) A controller or processor is not in violation of this chapter if:
586 (a) the controller or processor discloses personal data to a third party controller or
587 processor in compliance with this chapter;
588 (b) the third party processes the personal data in violation of this chapter; and
589 (c) the disclosing controller or processor did not have actual knowledge of the third
590 party's intent to commit a violation of this chapter.
591 (4) If a controller processes personal data under an exemption described in Subsection
592 (1), the controller bears the burden of demonstrating that the processing qualifies for the
593 exemption.
594 (5) Nothing in this chapter requires a controller, processor, third party, or consumer to
595 disclose a trade secret.

596 Section 12. Section **13-61-305** is enacted to read:

597 **13-61-305. No private cause of action.**

598 A violation of this chapter does not provide a basis for, nor is a violation of this chapter
599 subject to, a private right of action under this chapter or any other law.

600 Section 13. Section **13-61-401** is enacted to read:

601 **Part 4. Enforcement**

602 **13-61-401. Investigative powers of division.**

603 (1) The division shall establish and administer a system to receive consumer
604 complaints regarding a controller or processor's alleged violation of this chapter.

605 (2) (a) The division may investigate a consumer complaint to determine whether the
606 controller or processor violated or is violating this chapter.

607 (b) If the director has reasonable cause to believe that substantial evidence exists that a
608 person identified in a consumer complaint is in violation of this chapter, the director shall refer
609 the matter to the attorney general.

610 (c) Upon request, the division shall provide consultation and assistance to the attorney
611 general in enforcing this chapter.

612 Section 14. Section **13-61-402** is enacted to read:

613 **13-61-402. Enforcement powers of the attorney general.**

614 (1) The attorney general has the exclusive authority to enforce this chapter.

615 (2) Upon referral from the division, the attorney general may initiate an enforcement
616 action against a controller or processor for a violation of this chapter.

617 (3) (a) At least 30 days before the day on which the attorney general initiates an
618 enforcement action against a controller or processor, the attorney general shall provide the
619 controller or processor:

620 (i) written notice identifying each provision of this chapter the attorney general alleges
621 the controller or processor has violated or is violating; and

622 (ii) an explanation of the basis for each allegation.

623 (b) The attorney general may not initiate an action if the controller or processor:

624 (i) cures the noticed violation within 30 days after the day on which the controller or
625 processor receives the written notice described in Subsection (3)(a); and

626 (ii) provides the attorney general an express written statement that:

627 (A) the violation has been cured; and

628 (B) no further violation of the cured violation will occur.

629 (c) The attorney general may initiate an action against a controller or processor who:

630 (i) fails to cure a violation after receiving the notice described in Subsection (3)(a); or

631 (ii) after curing a noticed violation and providing a written statement in accordance
632 with Subsection (3)(b), continues to violate this chapter.

633 (d) In an action described in Subsection (3)(c), the attorney general may recover:

634 (i) actual damages to the consumer; and

635 (ii) for each violation described in Subsection (3)(c), an amount not to exceed \$7,500.

636 (4) All money received from an action under this chapter shall be deposited into the
637 Consumer Privacy Account established in Section [13-61-403](#).

638 (5) If more than one controller or processor are involved in the same processing in
639 violation of this chapter, the liability for the violation shall be allocated among the controllers
640 or processors according to the principles of comparative fault.

641 Section 15. Section **13-61-403** is enacted to read:

642 **13-61-403. Consumer Privacy Restricted Account.**

643 (1) There is created a restricted account known as the "Consumer Privacy Account."

644 (2) The account shall be funded by money received through civil enforcement actions
645 under this chapter.

646 (3) Upon appropriation, the division or the attorney general may use money deposited
647 into the account for:

648 (a) investigation and administrative costs incurred by the division in investigating
649 consumer complaints alleging violations of this chapter;

650 (b) recovery of costs and attorney fees accrued by the attorney general in enforcing this
651 chapter; and

652 (c) providing consumer and business education regarding:

653 (i) consumer rights under this chapter; and

654 (ii) compliance with the provisions of this chapter for controllers and processors.

655 (4) If the balance in the account exceeds \$4,000,000 at the close of any fiscal year, the
656 Division of Finance shall transfer the amount that exceeds \$4,000,000 into the General Fund.

657 Section 16. Section **13-61-404** is enacted to read:

658 **13-61-404. Attorney general report.**

659 (1) The attorney general and the division shall compile a report:

660 (a) evaluating the liability and enforcement provisions of this chapter, including the
661 effectiveness of the attorney general's and the division's efforts to enforce this chapter; and

662 (b) summarizing the data protected and not protected by this chapter including, with
663 reasonable detail, a list of the types of information that are publicly available from local, state,
664 and federal government sources.

665 (2) The attorney general and the division may update the report as new information
666 becomes available.

667 (3) The attorney general and the division shall submit the report to the Business and
668 Labor Interim Committee before July 1, 2025.

669 Section 17. **Effective date.**

670 This bill takes effect on December 31, 2023.