

Representative Jefferson Moss proposes the following substitute bill:

DATA PRIVACY AMENDMENTS

2024 GENERAL SESSION

STATE OF UTAH

Chief Sponsor: Jefferson Moss

Senate Sponsor: Kirk A. Cullimore

LONG TITLE

General Description:

This bill enacts the Government Data Privacy Act.

Highlighted Provisions:

This bill:

- ▶ defines terms;
- ▶ describes governmental entity duties related to personal data privacy, including:
 - breach notification;
 - limits on data collection and use; and
 - the ability to correct and access personal data;
- ▶ creates the state data privacy policy that outlines the broad data privacy goals for the state;
- ▶ creates the Utah Privacy Governing Board to recommend changes in the state data privacy policy;
- ▶ establishes the Office of Data Privacy to coordinate implementation of privacy protections; and
- ▶ renames the Personal Privacy Oversight Commission to the Utah Privacy Commission (commission) and amends the commission's duties.

Money Appropriated in this Bill:



26 None

27 **Other Special Clauses:**

28 None

29 **Utah Code Sections Affected:**

30 AMENDS:

31 **63A-12-115**, as enacted by Laws of Utah 2023, Chapter 173

32 **63C-24-101**, as enacted by Laws of Utah 2021, Chapter 155

33 **63C-24-102**, as last amended by Laws of Utah 2023, Chapter 16

34 **63C-24-201**, as enacted by Laws of Utah 2021, Chapter 155

35 **63C-24-202**, as last amended by Laws of Utah 2023, Chapter 173

36 **67-3-13**, as last amended by Laws of Utah 2023, Chapters 16, 173 and 435

37 ENACTS:

38 **63A-19-101**, Utah Code Annotated 1953

39 **63A-19-102**, Utah Code Annotated 1953

40 **63A-19-201**, Utah Code Annotated 1953

41 **63A-19-202**, Utah Code Annotated 1953

42 **63A-19-301**, Utah Code Annotated 1953

43 **63A-19-302**, Utah Code Annotated 1953

44 **63A-19-401**, Utah Code Annotated 1953

45 **63A-19-402**, Utah Code Annotated 1953

46 **63A-19-403**, Utah Code Annotated 1953

47 **63A-19-404**, Utah Code Annotated 1953

48 **63A-19-405**, Utah Code Annotated 1953

49 **63A-19-406**, Utah Code Annotated 1953

50 **63A-19-501**, Utah Code Annotated 1953

51 **63A-19-601**, Utah Code Annotated 1953

52 REPEALS:

53 **67-1-17**, as last amended by Laws of Utah 2023, Chapter 173



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

56 Section 1. Section **63A-12-115** is amended to read:

57 **63A-12-115. Privacy annotation for records series -- Requirements -- Content.**

58 (1) (a) Before January 1, [~~2026~~] 2027, an executive branch agency shall, for each
59 record series that the executive branch agency collects, maintains, or uses, evaluate the record
60 series and make a privacy annotation that completely and accurately complies with Subsection
61 (2) and the rules described in Subsection 63A-12-104(2)(e).

62 (b) Beginning on January 1, [~~2026~~] 2027, an executive branch agency may not collect,
63 maintain, or use personal identifying information unless the record series for which the
64 personal identifying information is collected, maintained, or used includes a privacy annotation
65 that completely and accurately complies with Subsection (2) and the rules described in
66 Subsection 63A-12-104(2)(e).

67 (2) A privacy annotation shall include the following:

68 (a) if the record series does not include personal identifying information, a statement
69 indicating that the record series does not include personal identifying information; or

70 (b) if the record series includes personal identifying information:

71 (i) an inventory of the personal identifying information included in the record series;
72 and

73 (ii) for the personal identifying information described in Subsection (2)(b)(i):

74 (A) the purpose for which the executive branch agency collects, keeps, or uses the
75 personal identifying information;

76 (B) a citation to the executive branch agency's legal authority for collecting, keeping, or
77 using the personal identifying information; and

78 (C) any other information required by state archives by rule under Subsection
79 63A-12-104(2)(e).

80 Section 2. Section **63A-19-101** is enacted to read:

81 **CHAPTER 19. GOVERNMENT DATA PRIVACY ACT**

82 **Part 1. General Provisions -- State Data Privacy Policy**

83 **63A-19-101. Definitions.**

84 As used in this chapter:

85 (1) "Chief privacy officer" means the individual appointed under Section 63A-19-302.

86 (2) "Commission" means the Utah Privacy Commission established in Section

87 63C-24-102.

88 (3) "Cyber Center" means the Utah Cyber Center created in Section [63A-16-510](#).

89 (4) "Data breach" means the unauthorized access, acquisition, disclosure, loss of
90 access, or destruction of personal data held by a governmental entity, unless the governmental
91 entity concludes, according to standards established by the Cyber Center, that there is a low
92 probability that personal data has been compromised.

93 (5) "Designated governmental entity" means the same as that term is defined in Section
94 [67-3-13](#).

95 (6) "Governing board" means the Utah Privacy Governing Board established in Section
96 [63A-19-201](#).

97 (7) "Governmental entity" means the same as that term is defined in Section
98 [63G-2-103](#).

99 (8) "High risk processing activities" means a governmental entity's processing of
100 personal data that may result in a significant compromise to an individual's privacy interests,
101 based on factors that include:

102 (a) the sensitivity of the personal data processed;

103 (b) the amount of personal data being processed;

104 (c) the individual's ability to consent to the processing of personal data; and

105 (d) risks of unauthorized access or use.

106 (9) "Individual" means the same as that term is defined in Section [63G-2-103](#).

107 (10) "Legal guardian" means:

108 (a) the parent of a minor; or

109 (b) an individual appointed by a court to be the guardian of a minor or incapacitated
110 person and given legal authority to make decisions regarding the person or property of the
111 minor or incapacitated person.

112 (11) "Office" means the Office of Data Privacy created in Section [63A-19-301](#).

113 (12) "Ombudsperson" means the data privacy ombudsperson appointed under Section
114 [63A-19-501](#).

115 (13) "Personal data" means information that is linked or can be reasonably linked to an
116 identified individual or an identifiable individual.

117 (14) "Process" or "processing" means any operation or set of operations performed on
118 personal data, including collection, recording, organization, structuring, storage, adaptation,

119 alteration, access, retrieval, consultation, use, disclosure by transmission, transfer,
120 dissemination, alignment, combination, restriction, erasure, or destruction.

121 (15) "Record" means the same as that term is defined in Section 63G-2-103.

122 (16) "Record series" means the same as that term is defined in Section 63G-2-103.

123 (17) "Retention schedule" means a governmental entity's schedule for the retention or
124 disposal of records that has been approved by the Records Management Committee pursuant to
125 Section 63A-12-113.

126 (18) (a) "Sell" means an exchange of personal data for monetary consideration by a
127 governmental entity to a third party.

128 (b) "Sell" does not include a fee:

129 (i) charged by a governmental entity for access to a record; or

130 (ii) assessed in accordance with an approved fee schedule.

131 (19) (a) "State agency" means the following entities that are under the direct
132 supervision and control of the governor or the lieutenant governor:

133 (i) a department;

134 (ii) a commission;

135 (iii) a board;

136 (iv) a council;

137 (v) an institution;

138 (vi) an officer;

139 (vii) a corporation;

140 (viii) a fund;

141 (ix) a division;

142 (x) an office;

143 (xi) a committee;

144 (xii) an authority;

145 (xiii) a laboratory;

146 (xiv) a library;

147 (xv) a bureau;

148 (xvi) a panel;

149 (xvii) another administrative unit of the state; or

- 150 (xviii) an agent of an entity described in Subsections (19)(a)(i) through (xvii).
- 151 (b) "State agency" does not include:
- 152 (i) the legislative branch;
- 153 (ii) the judicial branch;
- 154 (iii) an executive branch agency within the Office of the Attorney General, the state
- 155 auditor, the state treasurer, or the State Board of Education; or
- 156 (iv) an independent entity.

157 (20) "State privacy officer" means the individual described in Section [67-3-13](#).

158 Section 3. Section **63A-19-102** is enacted to read:

159 **63A-19-102. State data privacy policy.**

160 It is the policy of Utah that:

- 161 (1) an individual has a fundamental interest in and inherent expectation of privacy
- 162 regarding the personal data that the individual provides to a governmental entity;
- 163 (2) a governmental entity shall act in a manner respecting personal data provided to the
- 164 governmental entity that is consistent with the interests and expectations described in
- 165 Subsection (1);
- 166 (3) the state shall encourage innovation to enhance the ability of a governmental entity
- 167 to:
- 168 (a) protect the privacy of an individual's personal data;
- 169 (b) provide clear notice to an individual regarding the governmental entity's processing
- 170 of the individual's personal data;
- 171 (c) process personal data only for specified, lawful purposes and only process the
- 172 minimum amount of an individual's personal data necessary to achieve those purposes;
- 173 (d) implement appropriate consent mechanisms regarding the uses of an individual's
- 174 personal data;
- 175 (e) provide an individual with the ability to access, control, and request corrections to
- 176 the individual's personal data held by a governmental entity;
- 177 (f) maintain appropriate safeguards to protect the confidentiality, integrity, and
- 178 availability of personal data;
- 179 (g) account for compliance with privacy related laws, rules, and regulations that are
- 180 specific to a particular governmental entity, program, or personal data; and

- 181 (h) meet a governmental entity's and an individual's business and service needs;
- 182 (4) the state shall promote training and education programs for employees of
- 183 governmental entities focused on:
- 184 (a) data privacy best practices, obligations, and responsibilities; and
- 185 (b) the overlapping relationship with privacy, records management, and security; and
- 186 (5) the state shall promote consistent terminology in data privacy requirements across
- 187 governmental entities.

188 Section 4. Section **63A-19-201** is enacted to read:

189 **Part 2. Utah Privacy Governing Board**

190 **63A-19-201. Utah Privacy Governing Board.**

- 191 (1) There is created the Utah Privacy Governing Board.
- 192 (2) The governing board shall be composed of five members as follows:
- 193 (a) the governor, or the governor's designee;
- 194 (b) the president of the Senate, or the president's designee;
- 195 (c) the speaker of the House of Representatives, or the speaker's designee;
- 196 (d) the attorney general, or the attorney general's designee; and
- 197 (e) the state auditor, or the state auditor's designee.
- 198 (3) (a) A majority of the members of the governing board is a quorum.
- 199 (b) The action of a majority of a quorum constitutes an action of the governing board.
- 200 (4) The governor, or the governor's designee is chair of the governing board.
- 201 (5) The governing board shall meet at least two times a year.
- 202 (6) The governing board may recommend specific matters to the state auditor under

203 Section **63A-19-601.**

- 204 (7) The office shall provide staff and support to the governing board.

205 Section 5. Section **63A-19-202** is enacted to read:

206 **63A-19-202. Governing board duties.**

- 207 (1) The governing board shall:
- 208 (a) recommend changes to the state data privacy policy;
- 209 (b) by July 1 of each year, approve the data privacy agenda items for the commission
- 210 and make recommendations for additional items for the data privacy agenda;
- 211 (c) hear issues raised by the ombudsperson regarding existing governmental entity

243 data types, and maturity levels regarding privacy practices;
244 (b) review statutory provisions related to governmental data privacy and records
245 management to:
246 (i) identify conflicts and gaps in data privacy law;
247 (ii) standardize language; and
248 (iii) consult impacted agencies and the attorney general regarding findings and
249 proposed amendments;
250 (c) work with state agencies to study, research, and identify:
251 (i) additional privacy requirements that are feasible for state agencies;
252 (ii) potential remedies and accountability mechanisms for non-compliance of a state
253 agency;
254 (iii) ways to expand individual control and rights with respect to personal data held by
255 state agencies; and
256 (iv) resources needed to develop, implement, and improve privacy programs;
257 (d) monitor high-risk data processing activities within state agencies;
258 (e) receive information from state agencies regarding the sale, sharing, and processing
259 personal data;
260 (f) coordinate with the Cyber Center to develop an incident response plan for data
261 breaches affecting governmental entities;
262 (g) coordinate with the state archivist to incorporate data privacy practices into records
263 management;
264 (h) coordinate with the state archivist to incorporate data privacy training into the
265 trainings described in Section 63A-12-110; and
266 (i) create a data privacy training program for employees of governmental entities.
267 (4) The data privacy training program described in Subsection (3)(i) shall be made
268 available to all governmental entities, and shall be designed to provide instruction regarding:
269 (a) data privacy best practices, obligations, and responsibilities; and
270 (b) the relationship between privacy, records management, and security.
271 (5) (a) Except as provided in Subsection (5)(b), an employee of a state agency shall
272 complete the data privacy training program described in Subsection (3)(i):
273 (i) within 30 days of beginning employment; and

274 (ii) at least once in each calendar year.

275 (b) An employee of a state agency that does not have access to personal data as part of
276 the employee's work duties is not required to complete the data privacy training program
277 described in Subsection (3)(i).

278 (c) Each state agency is responsible for monitoring completion of data privacy training
279 by the state agency's employees.

280 (6) To the extent that resources permit, the office may provide expertise and assistance
281 to governmental entities for high risk data processing activities.

282 Section 7. Section **63A-19-302** is enacted to read:

283 **63A-19-302. Chief privacy officer -- Appointment -- Powers -- Reporting.**

284 (1) The governor shall, with the advice and consent of the Senate, appoint a chief
285 privacy officer.

286 (2) The chief privacy officer is the director of the office.

287 (3) The chief privacy officer:

288 (a) shall exercise all powers given to and perform all duties imposed on the office;

289 (b) has administrative authority over the office;

290 (c) may make changes in office personnel and service functions under the chief privacy
291 officer's administrative authority;

292 (d) may authorize a designee to assist with the chief privacy officer's responsibilities;
293 and

294 (e) shall report annually, on or before October 1, to the Judiciary Interim Committee
295 regarding:

296 (i) recommendations for legislation to address data privacy concerns; and

297 (ii) reports received from state agencies regarding the sale or sharing of personal data
298 provided under Subsection [63A-19-401\(2\)\(f\)\(ii\)](#).

299 Section 8. Section **63A-19-401** is enacted to read:

300 **Part 4. Duties of Governmental Entities**

301 **63A-19-401. Duties of governmental entities.**

302 (1) (a) Except as provided in Subsections (1)(b) and (c), a governmental entity shall
303 comply with the requirements of this part.

304 (b) (i) If a governmental entity or a contractor described in Subsection (4)(a) is subject

305 to a more restrictive or ~~more~~ specific provision of law than found in this part, the
 305a governmental
 306 entity ~~or contractor~~ shall comply with the more restrictive or ~~more~~ specific
 306a provision of law.

307 (ii) For purposes of Subsection (1)(b)(i), Title 63G, Chapter 2, Government Records
 308 Access and Management Act, is a more ~~restrictive and~~ specific provision of law ~~and shall control over the provisions of this part~~ .

309 (c) A governmental entity that is exempt under Section [63G-2-702](#), [63G-2-703](#), or
 310 [63G-2-704](#) from complying with the requirements in Title 63G, Chapter 2, Part 6, Collection of
 311 Information and Accuracy of Records, is exempt from complying with the requirements in
 312 Sections [63A-19-402](#), [63A-19-403](#), and [63A-19-404](#).

313 (2) A governmental entity:

314 (a) shall implement and maintain a privacy program before May 1, 2025, that includes
 315 the governmental entity's policies, practices, and procedures for the process of personal data;

316 (b) shall provide notice to an individual or the legal guardian of an individual, if the
 317 individual's personal data is affected by a data breach, in accordance with Section [63A-19-406](#);

318 (c) shall obtain and process only the minimum amount of personal data reasonably
 319 necessary to efficiently achieve a specified purpose;

320 (d) shall meet the requirements of this part for all processing activities implemented by
 321 a governmental entity after May 1, 2024;

322 (e) shall for any processing activity implemented before May 1, 2024, as soon as is
 323 reasonably practicable, but no later than January 1, 2027:

324 (i) identify any non-compliant processing activity;

325 (ii) document the non-compliant processing activity; and

326 (iii) prepare a strategy for bringing the non-compliant processing activity into
 327 compliance with this part;

328 (f) may not establish, maintain, or use undisclosed or covert surveillance of individuals
 329 unless permitted by law;

330 (g) may not sell personal data unless expressly required by law;

331 (h) may not share personal data unless permitted by law;

332 (i) (i) that is a designated governmental entity, shall annually report to the state privacy
 333 officer:

334 (A) the types of personal data the designated governmental entity currently shares or
 335 sells;

336 (B) the basis for sharing or selling the personal data; and
337 (C) the classes of persons and the governmental entities that receive the personal data
338 from the designated governmental entity; and

339 (ii) that is a state agency, shall annually report to the chief privacy officer:

340 (A) the types of personal data the state agency currently shares or sells;

341 (B) the basis for sharing or selling the personal data; and

342 (C) the classes of persons and the governmental entities that receive the personal data
343 from the state agency; and

344 (j) (i) except as provided in Subsection (3), an employee of a governmental entity shall
345 complete a data privacy training program:

346 (A) within 30 days after beginning employment; and

347 (B) at least once in each calendar year; and

348 (k) is responsible for monitoring completion of data privacy training by the
349 governmental entity's employees.

350 (3) An employee of a governmental entity that does not have access to personal data of
351 individuals as part of the employee's work duties is not required to complete a data privacy
352 training program described in Subsection (2)(j)(i).

353 (4) (a) A contractor that enters into or renews an agreement with a governmental entity
354 after May 1, 2024, and processes or has access to personal data as a part of the contractor's
355 duties under the agreement, is subject to the requirements of this chapter with regard to the
356 personal data processed or accessed by the contractor to the same extent as required of the
357 governmental entity.

358 (b) An agreement under Subsection (4)(a) shall require the contractor to comply with
359 the requirements of this chapter ~~with regard to the personal data processed or accessed by~~
359a ~~the contractor as a part of the contractor's duties under the agreement~~ to the same extent
359b as ~~required of~~ the governmental entity.

360 (c) The requirements under Subsections (4)(a) and (b) are in addition to and do not
361 replace any other requirements or liability that may be imposed for the contractor's violation of
362 other laws protecting privacy rights or government records.

363 Section 9. Section **63A-19-402** is enacted to read:

364 **63A-19-402. General governmental privacy requirements -- Personal data request**
365 **notice.**

366 (1) A governmental entity shall provide a personal data request notice to an individual,

367 or the legal guardian of an individual, from whom the governmental entity requests or collects
368 personal data.

369 (2) The personal data request notice described in Subsection (1) shall include:

370 (a) the reasons the individual is asked to provide the personal data;

371 (b) the intended purposes and uses of the personal data;

372 (c) the consequences for refusing to provide the personal data;

373 (d) the classes of persons and entities that:

374 (i) share the personal data with the governmental entity; or

375 (ii) receive the personal data from the governmental entity on a regular or contractual
376 basis; and

377 (e) the record series in which the personal data is or will be included, if applicable.

378 (3) The governmental entity shall provide the personal data request notice by:

379 (a) posting the personal data request notice in a prominent place where the

380 governmental entity collects the personal data;

381 (b) including the personal data request notice as part of any document or form used by
382 the governmental entity to collect the personal data; or

383 (c) conspicuously linking to or displaying a QR code linked to an electronic version of
384 the personal data request notice as part of any document or form used by the governmental
385 entity to collect the personal data.

386 (4) The personal data request notice required by this section is in addition to, and does
387 not supersede, any other notice requirement otherwise applicable to the governmental entity.

388 (5) The governmental entity shall, upon request, provide the personal data request
389 notice to an individual, or the legal guardian of an individual, regarding personal data
390 previously furnished by that individual.

391 (6) The governmental entity may only use personal data furnished by an individual for
392 the purposes identified in the personal data request notice provided to that individual.

393 Section 10. Section **63A-19-403** is enacted to read:

394 **63A-19-403. Procedure to request amendment or correction of personal data.**

395 (1) A governmental entity that collects personal data shall provide a procedure by
396 which an individual or legal guardian of an individual may request an amendment or correction
397 of personal data that has been furnished to the governmental entity.

398 (2) The procedure by which an individual or legal guardian of an individual may
399 request an amendment or correction shall comply with all applicable laws and regulations to
400 which the personal data at issue and to which the governmental entity is subject.

401 (3) The procedure to request an amendment or correction described in this section does
402 not obligate the governmental entity to make the requested amendment or correction.

403 Section 11. Section **63A-19-404** is enacted to read:

404 **63A-19-404. Retention and disposition of personal data.**

405 (1) A governmental entity that collects personal data shall retain and dispose of the
406 personal data in accordance with a documented record retention schedule.

407 (2) Compliance with Subsection (1) does not exempt a governmental entity from
408 complying with other applicable laws or regulations related to retention or disposition of
409 specific personal data held by that governmental entity.

410 Section 12. Section **63A-19-405** is enacted to read:

411 **63A-19-405. Data breach notification to the Cyber Center and the Office of the**
412 **Attorney General.**

413 (1) (a) A governmental entity that identifies a data breach affecting 500 or more
414 individuals shall notify the Cyber Center and the attorney general of the data breach.

415 (b) In addition to the notification required by Subsection (1)(a), a governmental entity
416 that identifies the unauthorized access, acquisition, disclosure, loss of access, or destruction of
417 data that compromises the security, confidentiality, availability, or integrity of the computer
418 systems used or information maintained by the governmental entity shall notify the Cyber
419 Center.

420 (2) The notification under Subsection (1) shall:

421 (a) be made without unreasonable delay, but no later than five days from the discovery
422 of the data breach; and

423 (b) include the following information:

424 (i) the date and time the data breach occurred;

425 (ii) the date the data breach was discovered;

426 (iii) a short description of the data breach that occurred;

427 (iv) the means by which access was gained to the system, computer, or network;

428 (v) the individual or entity who perpetrated the data breach;

429 (vi) steps the governmental entity is or has taken to mitigate the impact of the data
430 breach; and

431 (vii) any other details requested by the Cyber Center.

432 (3) For a data breach under Subsection (1)(a), the governmental entity shall provide the
433 following information to the Cyber Center and the attorney general in addition to the
434 information required under Subsection (2)(b):

435 (a) the total number of people affected by the data breach, including the total number
436 of Utah residents affected; and

437 (b) the type of personal data involved in the data breach.

438 (4) If the information required by Subsection (2)(b) is not available within five days of
439 discovering the breach, the governmental entity shall provide as much of the information
440 required under Subsection (2)(b) as is available and supplement the notification with additional
441 information as soon as the information becomes available.

442 (5) (a) A governmental entity that experiences a data breach affecting fewer than 500
443 individuals shall create an internal incident report containing the information in Subsection
444 (2)(b) as soon as practicable and shall provide additional information as the information
445 becomes available.

446 (b) A governmental entity shall provide to the Cyber Center:

447 (i) an internal incident report described in Subsection (5)(a) upon request of the Cyber
448 Center; and

449 (ii) an annual report logging all of the governmental entity's data breach incidents
450 affecting fewer than 500 individuals.

451 Section 13. Section **63A-19-406** is enacted to read:

452 **63A-19-406. Data breach notice to individuals affected by data breach.**

453 (1) A governmental entity shall provide a data breach notice to an individual or legal
454 guardian of an individual affected by the data breach:

455 (a) after determining the scope of the data breach;

456 (b) after restoring the reasonable integrity of the affected system, if necessary; and

457 (c) without unreasonable delay except as provided in Subsection (1)(b).

458 (2) A governmental entity shall delay providing notification under Subsection (1) at the
459 request of a law enforcement agency that determines that notification may impede a criminal

460 investigation, until such time as the law enforcement agency informs the governmental entity
461 that notification will no longer impede the criminal investigation.

462 (3) The data breach notice to an affected individual shall include:

463 (a) a description of the data breach;

464 (b) the individual's personal data that was accessed or may have been accessed;

465 (c) steps the governmental entity is taking or has taken to mitigate the impact of the
466 data breach;

467 (d) recommendations to the individual on how to protect themselves from identity theft
468 and other financial losses; and

469 (e) any other language required by the Cyber Center.

470 (4) Unless the governmental entity reasonably believes that providing notification

471 would pose a threat to the safety of an individual, or unless an individual has designated to the
472 governmental entity a preferred method of communication, a governmental entity shall provide
473 notice by:

474 (a) (i) email, if reasonably available and allowed by law; or

475 (ii) mail; and

476 (b) one of the following methods, if the individual's contact information is reasonably
477 available and the method is allowed by law:

478 (i) text message with a summary of the data breach notice and instructions for
479 accessing the full notice; or

480 (ii) telephone message with a summary of the data breach notice and instructions for
481 accessing the full data breach notice.

482 (5) A governmental entity shall also provide a data breach notice in a manner that is
483 reasonably calculated to have the best chance of being received by the affected individual or
484 the legal guardian of an individual, such as through a press release, posting on appropriate
485 social media accounts, or publishing notice in a newspaper of general circulation when:

486 (a) a data breach affects more than 500 individuals; and

487 (b) a governmental entity is unable to obtain an individual's contact information to
488 provide notice for any method listed in Subsection (4).

489 Section 14. Section **63A-19-501** is enacted to read:

490 **Part 5. Data Privacy Ombudsperson**

491 **63A-19-501. Data privacy ombudsperson.**

492 (1) The governor shall appoint a data privacy ombudsperson with the advice of the
493 governing board.

494 (2) The ombudsperson shall:

495 (a) be familiar with the provisions of:

496 (i) this chapter;

497 (ii) Chapter 12, Division of Archives and Records Service and Management of
498 Government Records; and

499 (iii) Title 63G, Chapter 2, Government Records Access and Management Act; and

500 (b) serve as a resource for an individual who is making or responding to a complaint
501 about a governmental entity's data privacy practice.

502 (3) The ombudsperson may, upon request by a governmental entity or individual,
503 mediate data privacy disputes between individuals and governmental entities.

504 (4) After consultation with the chief privacy officer or the state privacy officer, the
505 ombudsperson may raise issues and questions before the governing board regarding serious and
506 repeated violations of data privacy from:

507 (a) a specific governmental entity; or

508 (b) widespread governmental entity data privacy practices.

509 Section 15. Section **63A-19-601** is enacted to read:

510 **Part 6. Remedies**

511 **63A-19-601. Enforcement.**

512 (1) Upon instruction by the board, the state auditor shall:

513 (a) investigate alleged violations of this chapter by a governmental entity;

514 (b) provide notice to the relevant governmental entity of an alleged violation of this
515 chapter; and

516 (c) for a violation that the state auditor substantiates, provide an opportunity for the
517 governmental entity to cure the violation within 30 days.

518 (2) If a governmental entity fails to cure a violation as provided in Subsection (1)(c),
519 the state auditor shall report the governmental entity's failure:

520 (a) for a designated governmental entity, to the attorney general for enforcement under
521 Subsection (3); and

522 (b) for a state agency, to the Legislative Management Committee.

523 (3) After referral by the state auditor under Subsection (2)(a), the attorney general may
524 file an action in district court to:

525 (a) enjoin a designated governmental entity from violating this chapter; or

526 (b) require a designated governmental entity to comply with this chapter.

527 Section 16. Section **63C-24-101** is amended to read:

528 **CHAPTER 24. UTAH PRIVACY COMMISSION**

529 **Part 1. General Provisions**

530 **63C-24-101. Title.**

531 This chapter is known as the [~~"Personal Privacy Oversight]~~ "Utah Privacy
532 Commission."

533 Section 17. Section **63C-24-102** is amended to read:

534 **63C-24-102. Definitions.**

535 As used in this chapter:

536 (1) "Commission" means the [~~Personal Privacy Oversight]~~ Utah Privacy Commission
537 created in Section [63C-24-201](#).

538 (2) "Governing board" means the Utah Privacy Governing Board created in Section
539 [63A-9-201](#).

540 (3) "Governmental entity" means the same as that term is defined in Section
541 [63G-2-103](#).

542 [~~(2)(a) "Government entity" means the state, a county, a municipality, a higher~~
543 ~~education institution, a special district, a special service district, a school district, an~~
544 ~~independent entity, or any other political subdivision of the state or an administrative subunit of~~
545 ~~any political subdivision, including a law enforcement entity.]~~

546 [~~(b) "Government entity" includes an agent of an entity described in Subsection (2)(a).]~~

547 [~~(3)]~~ (4) "Independent entity" means the same as that term is defined in Section
548 [63E-1-102](#).

549 (5) "Office" means the Office of Data Privacy created in Section [63A-19-301](#).

550 [~~(4)]~~ (6) [(a)] "Personal data" means [~~any information relating to an identified or~~
551 ~~identifiable individual]~~ the same as that term is defined in Section [63A-19-101](#).

552 [~~(b) "Personal data" includes personally identifying information.]~~

584 (b) The initial appointments of members described in Subsections (2)(b)(i) through
585 (b)(iii), (2)(c)(iv) through (c)(v), and (2)(d)(ii) shall be for two-year terms.

586 (c) When the term of a current member expires, a member shall be reappointed or a
587 new member shall be appointed in accordance with Subsection (2).

588 (4) (a) When a vacancy occurs in the membership for any reason, a replacement shall
589 be appointed in accordance with Subsection (2) for the unexpired term.

590 (b) A member whose term has expired may continue to serve until a replacement is
591 appointed.

592 (5) The commission shall select officers from the commission's members as the
593 commission finds necessary.

594 (6) (a) A majority of the members of the commission is a quorum.

595 (b) The action of a majority of a quorum constitutes an action of the commission.

596 (7) A member may not receive compensation or benefits for the member's service but
597 may receive per diem and travel expenses incurred as a member of the commission at the rates
598 established by the Division of Finance under:

599 (a) Sections [63A-3-106](#) and [63A-3-107](#); and

600 (b) rules made by the Division of Finance in accordance with Sections [63A-3-106](#) and
601 [63A-3-107](#).

602 (8) A member shall refrain from participating in a review of:

603 (a) an entity of which the member is an employee; or

604 (b) a technology in which the member has a financial interest.

605 (9) The state auditor shall provide staff and support to the commission.

606 (10) The commission shall meet up to [~~seven~~] 12 times a year to accomplish the duties
607 described in Section [63C-24-202](#).

608 Section 19. Section [63C-24-202](#) is amended to read:

609 **[63C-24-202. Commission duties.](#)**

610 (1) The commission shall:

611 (a) annually develop a data privacy agenda that identifies for the upcoming year:

612 (i) governmental entity privacy practices to be reviewed by the commission;

613 (ii) educational and training materials that the commission intends to develop;

614 (iii) any other items related to data privacy the commission intends to study; and

615 (iv) best practices and guiding principles that the commission plans to develop related
616 to government privacy practices;

617 (b) develop guiding standards and best practices with respect to government privacy
618 practices;

619 ~~[(b)]~~ (c) develop educational and training materials that include information about:

620 (i) the privacy implications and civil liberties concerns of the privacy practices of
621 government entities;

622 (ii) best practices for government collection and retention policies regarding personal
623 data; and

624 (iii) best practices for government personal data security standards; [and]

625 ~~[(e)]~~ (d) review the privacy implications and civil liberties concerns of government
626 privacy practices[-]; and

627 (e) provide the data privacy agenda to the governing board by May 1 of each year.

628 (2) The commission may, in addition to the approved items in the data privacy agenda
629 prepared under Subsection (1)(a):

630 (a) review specific government privacy practices as referred to the commission by the
631 chief privacy officer described in Section ~~[67-1-17]~~ [63A-19-302](#) or the state privacy officer
632 described in Section [67-3-13](#); [and]

633 (b) review a privacy practice not accounted for in the data privacy agenda only upon
634 referral by the chief privacy officer or the state privacy officer in accordance with Subsection
635 [63C-24-202\(2\)\(a\)](#);

636 (c) review and provide recommendations regarding consent mechanisms used by
637 governmental entities to collect personal information;

638 (d) develop and provide recommendations to the Legislature on how to balance
639 transparency and public access of public records against an individual's reasonable expectations
640 of privacy and data protection; and

641 ~~[(b)]~~ (e) develop recommendations for legislation regarding the guiding standards and
642 best practices the commission has developed in accordance with Subsection (1)(a).

643 (3) ~~[Annually]~~ At least annually, on or before October 1, the commission shall report to
644 the Judiciary Interim Committee:

645 (a) the results of any reviews the commission has conducted;

646 (b) the guiding standards and best practices described in Subsection ~~[(1)(a)]~~ (1)(b); and
647 (c) any recommendations for legislation the commission has developed in accordance
648 with Subsection ~~[(2)(b)]~~ (2)(c).

649 (4) At least annually, on or before June 1, the commission shall report to the governing
650 board regarding:

651 (a) governmental entity privacy practices the commission plans to review in the next
652 year;

653 (b) any educational and training programs the commission intends to develop in
654 relation to government data privacy best practices;

655 (c) results of the commission's data privacy practice reviews from the previous year;
656 and

657 (d) recommendations from the commission related to data privacy legislation,
658 standards, or best practices.

659 (5) The data privacy agenda detailed in Subsection (1)(a) does not add to or expand the
660 authority of the commission.

661 Section 20. Section **67-3-13** is amended to read:

662 **67-3-13. State privacy officer.**

663 (1) As used in this section:

664 (a) "Designated ~~[government]~~ governmental entity" means a ~~[government]~~
665 governmental entity that is not a state agency.

666 (b) "Independent entity" means the same as that term is defined in Section [63E-1-102](#).

667 (c) "Governmental entity" means the same as that term is defined in Section
668 [63G-2-103](#).

669 ~~[(c) (i) "Government entity" means the state, a county, a municipality, a higher~~
670 ~~education institution, a special district, a special service district, a school district, an~~
671 ~~independent entity, or any other political subdivision of the state or an administrative subunit of~~
672 ~~any political subdivision, including a law enforcement entity.]~~

673 ~~[(ii) "Government entity" includes an agent of an entity described in Subsection~~
674 ~~(1)(c)(i).]~~

675 (d) ~~[(i)]~~ "Personal data" means ~~[any information relating to an identified or identifiable~~
676 ~~individual.]~~ the same as that term is defined in Section [63A-19-101](#).

- 677 ~~[(ii) "Personal data" includes personally identifying information.]~~
- 678 (e) (i) "Privacy practice" means the acquisition, use, storage, or disposal of personal
679 data.
- 680 (ii) "Privacy practice" includes:
- 681 (A) a technology use related to personal data; and
- 682 (B) policies related to the protection, storage, sharing, and retention of personal data.
- 683 (f) (i) "State agency" means the following entities that are under the direct supervision
684 and control of the governor or the lieutenant governor:
- 685 (A) a department;
- 686 (B) a commission;
- 687 (C) a board;
- 688 (D) a council;
- 689 (E) an institution;
- 690 (F) an officer;
- 691 (G) a corporation;
- 692 (H) a fund;
- 693 (I) a division;
- 694 (J) an office;
- 695 (K) a committee;
- 696 (L) an authority;
- 697 (M) a laboratory;
- 698 (N) a library;
- 699 (O) a bureau;
- 700 (P) a panel;
- 701 (Q) another administrative unit of the state; or
- 702 (R) an agent of an entity described in Subsections (A) through (Q).
- 703 (ii) "State agency" does not include:
- 704 (A) the legislative branch;
- 705 (B) the judicial branch;
- 706 (C) an executive branch agency within the Office of the Attorney General, the state
707 auditor, the state treasurer, or the State Board of Education; or

- 708 (D) an independent entity.
- 709 (2) The state privacy officer shall:
- 710 (a) when completing the duties of this Subsection (2), focus on the privacy practices of
- 711 designated [~~government~~] governmental entities;
- 712 (b) compile information about government privacy practices of designated
- 713 [~~government~~] governmental entities;
- 714 (c) make public and maintain information about government privacy practices on the
- 715 state auditor's website;
- 716 (d) provide designated [~~government~~] governmental entities with educational and
- 717 training materials developed by the [~~Personal Privacy Oversight~~] Utah Privacy Commission
- 718 established in Section [63C-24-201](#) that include the information described in Subsection
- 719 [63C-24-202\(1\)\(b\)](#);
- 720 (e) implement a process to analyze and respond to requests from individuals for the
- 721 state privacy officer to review a designated [~~government~~] governmental entity's privacy
- 722 practice;
- 723 (f) identify annually which designated [~~government~~] governmental entities' privacy
- 724 practices pose the greatest risk to individual privacy and prioritize those privacy practices for
- 725 review;
- 726 (g) review each year, in as timely a manner as possible, the privacy practices that the
- 727 privacy officer identifies under Subsection (2)(e) or (2)(f) as posing the greatest risk to
- 728 individuals' privacy;
- 729 (h) when reviewing a designated [~~government~~] governmental entity's privacy practice
- 730 under Subsection (2)(g), analyze:
- 731 (i) details about the technology or the policy and the technology's or the policy's
- 732 application;
- 733 (ii) information about the type of data being used;
- 734 (iii) information about how the data is obtained, stored, shared, secured, and disposed;
- 735 (iv) information about with which persons the designated [~~government~~] governmental
- 736 entity shares the information;
- 737 (v) information about whether an individual can or should be able to opt out of the
- 738 retention and sharing of the individual's data;

- 739 (vi) information about how the designated [government] governmental entity
740 de-identifies or anonymizes data;
- 741 (vii) a determination about the existence of alternative technology or improved
742 practices to protect privacy; and
- 743 (viii) a finding of whether the designated [government] governmental entity's current
744 privacy practice adequately protects individual privacy; and
- 745 (i) after completing a review described in Subsections (2)(g) and (h), determine:
- 746 (i) each designated [government] governmental entity's use of personal data, including
747 the designated [government] governmental entity's practices regarding data:
- 748 (A) acquisition;
- 749 (B) storage;
- 750 (C) disposal;
- 751 (D) protection; and
- 752 (E) sharing;
- 753 (ii) the adequacy of the designated [government] governmental entity's practices in
754 each of the areas described in Subsection (2)(i)(i); and
- 755 (iii) for each of the areas described in Subsection (2)(i)(i) that the state privacy officer
756 determines to require reform, provide recommendations for reform to the designated
757 [government] governmental entity and the legislative body charged with regulating the
758 designated [government] governmental entity.
- 759 (3) (a) The legislative body charged with regulating a designated [government]
760 governmental entity that receives a recommendation described in Subsection (2)(i)(iii) shall
761 hold a public hearing on the proposed reforms:
- 762 (i) with a quorum of the legislative body present; and
- 763 (ii) within 90 days after the day on which the legislative body receives the
764 recommendation.
- 765 (b) (i) The legislative body shall provide notice of the hearing described in Subsection
766 (3)(a).
- 767 (ii) Notice of the public hearing and the recommendations to be discussed shall be
768 posted for the jurisdiction of the designated [government] governmental entity, as a class A
769 notice under Section [63G-30-102](#), for at least 30 days before the day on which the legislative

770 body will hold the public hearing.

771 (iii) Each notice required under Subsection (3)(b)(i) shall:

772 (A) identify the recommendations to be discussed; and

773 (B) state the date, time, and location of the public hearing.

774 (c) During the hearing described in Subsection (3)(a), the legislative body shall:

775 (i) provide the public the opportunity to ask questions and obtain further information
776 about the recommendations; and

777 (ii) provide any interested person an opportunity to address the legislative body with
778 concerns about the recommendations.

779 (d) At the conclusion of the hearing, the legislative body shall determine whether the
780 legislative body shall adopt reforms to address the recommendations and any concerns raised
781 during the public hearing.

782 (4) (a) Except as provided in Subsection (4)(b), if the chief privacy officer described in
783 Section ~~[67-1-17]~~ [63A-19-302](#) is not conducting reviews of the privacy practices of state
784 agencies, the state privacy officer may review the privacy practices of a state agency in
785 accordance with the processes described in this section.

786 (b) Subsection (3) does not apply to a state agency.

787 (5) The state privacy officer shall:

788 (a) quarterly report, to the ~~[Personal Privacy Oversight Commission]~~ Utah Privacy
789 Commission:

790 (i) recommendations for privacy practices for the commission to review; and

791 (ii) the information provided in Subsection (2)(i); and

792 (b) annually, on or before October 1, report to the Judiciary Interim Committee:

793 (i) the results of any reviews described in Subsection (2)(g), if any reviews have been
794 completed;

795 (ii) reforms, to the extent that the state privacy officer is aware of any reforms, that the
796 designated ~~[government]~~ governmental entity made in response to any reviews described in
797 Subsection (2)(g);

798 (iii) the information described in Subsection (2)(i);

799 (iv) reports received from designated governmental entities regarding the sale or
800 sharing of personal data provided under Subsection [63A-19-401\(2\)\(f\)\(i\)](#); and

801 [~~(iv)~~] (v) recommendations for legislation based on any results of a review described in
802 Subsection (2)(g).

803 Section 21. **Repealer.**

804 This bill repeals:

805 Section **67-1-17, Chief privacy officer.**

806 Section 22. **Effective date.**

807 This bill takes effect on May 1, 2024.