

**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

Cosponsors: Candice B. Pierucci

Kera Birkeland Judy Weeks Rohner

---

---

**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



25           ▶ renames the Personal Privacy Oversight Commission to the Utah Privacy  
26 Commission (commission) and amends the commission's duties.

27 **Money Appropriated in this Bill:**

28           None

29 **Other Special Clauses:**

30           This bill provides a coordination clause.

31 **Utah Code Sections Affected:**

32 AMENDS:

33           **63A-12-115**, as enacted by Laws of Utah 2023, Chapter 173

34           **63C-24-101**, as enacted by Laws of Utah 2021, Chapter 155

35           **63C-24-102**, as last amended by Laws of Utah 2023, Chapter 16

36           **63C-24-201**, as enacted by Laws of Utah 2021, Chapter 155

37           **63C-24-202**, as last amended by Laws of Utah 2023, Chapter 173

38           **67-3-13**, as last amended by Laws of Utah 2023, Chapters 16, 173 and 435

39 ENACTS:

40           **63A-19-101**, Utah Code Annotated 1953

41           **63A-19-102**, Utah Code Annotated 1953

42           **63A-19-201**, Utah Code Annotated 1953

43           **63A-19-202**, Utah Code Annotated 1953

44           **63A-19-301**, Utah Code Annotated 1953

45           **63A-19-302**, Utah Code Annotated 1953

46           **63A-19-401**, Utah Code Annotated 1953

47           **63A-19-402**, Utah Code Annotated 1953

48           **63A-19-403**, Utah Code Annotated 1953

49           **63A-19-404**, Utah Code Annotated 1953

50           **63A-19-405**, Utah Code Annotated 1953

51           **63A-19-406**, Utah Code Annotated 1953

52           **63A-19-501**, Utah Code Annotated 1953

53           **63A-19-601**, Utah Code Annotated 1953

54 REPEALS:

55           **67-1-17**, as last amended by Laws of Utah 2023, Chapter 173

56 **Utah Code Sections Affected By Coordination Clause:**

57 **63A-19-101**, as Utah Code Annotated 1953



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

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

61 **63A-12-115. Privacy annotation for records series -- Requirements -- Content.**

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

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

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

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

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

75 (i) an inventory of the personal identifying information included in the record series;

76 and

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

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

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

82 (C) any other information required by state archives by rule under Subsection  
83 **63A-12-104**(2)(e).

84 *The following section is affected by a coordination clause at the end of this bill.*

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

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

87 **Part 1. General Provisions -- State Data Privacy Policy**88 **63A-19-101. Definitions.**89 As used in this chapter:90 (1) "Chief privacy officer" means the individual appointed under Section [63A-19-302](#).91 (2) "Commission" means the Utah Privacy Commission established in Section  
92 [63C-24-102](#).93 (3) "Cyber Center" means the Utah Cyber Center created in Section [63A-16-510](#).94 (4) "Data breach" means the unauthorized access, acquisition, disclosure, loss of  
95 access, or destruction of personal data held by a governmental entity, unless the governmental  
96 entity concludes, according to standards established by the Cyber Center, that there is a low  
97 probability that personal data has been compromised.98 (5) "Designated governmental entity" means the same as that term is defined in Section  
99 [67-3-13](#).100 (6) "Governing board" means the Utah Privacy Governing Board established in Section  
101 [63A-19-201](#).102 (7) "Governmental entity" means the same as that term is defined in Section  
103 [63G-2-103](#).104 (8) "High risk processing activities" means a governmental entity's processing of  
105 personal data that may result in a significant compromise to an individual's privacy interests,  
106 based on factors that include:107 (a) the sensitivity of the personal data processed;108 (b) the amount of personal data being processed;109 (c) the individual's ability to consent to the processing of personal data; and110 (d) risks of unauthorized access or use.111 (9) "Individual" means the same as that term is defined in Section [63G-2-103](#).112 (10) "Legal guardian" means:113 (a) the parent of a minor; or114 (b) an individual appointed by a court to be the guardian of a minor or incapacitated  
115 person and given legal authority to make decisions regarding the person or property of the  
116 minor or incapacitated person.117 (11) "Office" means the Office of Data Privacy created in Section [63A-19-301](#).

118 (12) "Ombudsperson" means the data privacy ombudsperson appointed under Section  
119 63A-19-501.

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

122 (14) "Process" or "processing" means any operation or set of operations performed on  
123 personal data, including collection, recording, organization, structuring, storage, adaptation,  
124 alteration, access, retrieval, consultation, use, disclosure by transmission, transfer,  
125 dissemination, alignment, combination, restriction, erasure, or destruction.

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

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

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

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

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

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

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

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

138 (i) a department;

139 (ii) a commission;

140 (iii) a board;

141 (iv) a council;

142 (v) an institution;

143 (vi) an officer;

144 (vii) a corporation;

145 (viii) a fund;

146 (ix) a division;

147 (x) an office;

148 (xi) a committee;

- 149           (xii) an authority;
- 150           (xiii) a laboratory;
- 151           (xiv) a library;
- 152           (xv) a bureau;
- 153           (xvi) a panel;
- 154           (xvii) another administrative unit of the state; or
- 155           (xviii) an agent of an entity described in Subsections (19)(a)(i) through (xvii).
- 156           (b) "State agency" does not include:
- 157           (i) the legislative branch;
- 158           (ii) the judicial branch;
- 159           (iii) an executive branch agency within the Office of the Attorney General, the state
- 160 auditor, the state treasurer, or the State Board of Education; or
- 161           (iv) an independent entity.
- 162           (20) "State privacy officer" means the individual described in Section [67-3-13](#).
- 163           Section 3. Section **63A-19-102** is enacted to read:
- 164           **63A-19-102. State data privacy policy.**
- 165           It is the policy of Utah that:
- 166           (1) an individual has a fundamental interest in and inherent expectation of privacy
- 167 regarding the personal data that the individual provides to a governmental entity;
- 168           (2) a governmental entity shall act in a manner respecting personal data provided to the
- 169 governmental entity that is consistent with the interests and expectations described in
- 170 Subsection (1);
- 171           (3) the state shall encourage innovation to enhance the ability of a governmental entity
- 172 to:
- 173           (a) protect the privacy of an individual's personal data;
- 174           (b) provide clear notice to an individual regarding the governmental entity's processing
- 175 of the individual's personal data;
- 176           (c) process personal data only for specified, lawful purposes and only process the
- 177 minimum amount of an individual's personal data necessary to achieve those purposes;
- 178           (d) implement appropriate consent mechanisms regarding the uses of an individual's
- 179 personal data;

180 (e) provide an individual with the ability to access, control, and request corrections to  
181 the individual's personal data held by a governmental entity;

182 (f) maintain appropriate safeguards to protect the confidentiality, integrity, and  
183 availability of personal data;

184 (g) account for compliance with privacy related laws, rules, and regulations that are  
185 specific to a particular governmental entity, program, or personal data; and

186 (h) meet a governmental entity's and an individual's business and service needs;

187 (4) the state shall promote training and education programs for employees of  
188 governmental entities focused on:

189 (a) data privacy best practices, obligations, and responsibilities; and

190 (b) the overlapping relationship with privacy, records management, and security; and

191 (5) the state shall promote consistent terminology in data privacy requirements across  
192 governmental entities.

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

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

195 **63A-19-201. Utah Privacy Governing Board.**

196 (1) There is created the Utah Privacy Governing Board.

197 (2) The governing board shall be composed of five members as follows:

198 (a) the governor, or the governor's designee;

199 (b) the president of the Senate, or the president's designee;

200 (c) the speaker of the House of Representatives, or the speaker's designee;

201 (d) the attorney general, or the attorney general's designee; and

202 (e) the state auditor, or the state auditor's designee.

203 (3) (a) A majority of the members of the governing board is a quorum.

204 (b) The action of a majority of a quorum constitutes an action of the governing board.

205 (4) The governor, or the governor's designee is chair of the governing board.

206 (5) The governing board shall meet at least two times a year.

207 (6) The governing board may recommend specific matters to the state auditor under

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

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

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

211 63A-19-202. Governing board duties.

212 (1) The governing board shall:

213 (a) recommend changes to the state data privacy policy;

214 (b) by July 1 of each year, approve the data privacy agenda items for the commission

215 and make recommendations for additional items for the data privacy agenda;

216 (c) hear issues raised by the ombudsperson regarding existing governmental entity

217 privacy practices;

218 (d) evaluate and recommend the appropriate:

219 (i) structure and placement for the office within state government; and

220 (ii) authority to be granted to the office, including any authority to make rules; and

221 (e) recommend funding mechanisms and strategies for governmental entities to enable

222 compliance with data privacy responsibilities, including:

223 (i) appropriations;

224 (ii) rates;

225 (iii) grants; and

226 (iv) internal service funds.

227 (2) In fulfilling the duties under this part, the governing board may receive and request

228 input from:

229 (a) governmental entities;

230 (b) elected officials;

231 (c) subject matter experts; and

232 (d) other stakeholders.

233 Section 6. Section **63A-19-301** is enacted to read:

234 **Part 3. Office of Data Privacy**

235 **63A-19-301. Office of Data Privacy.**

236 (1) There is created within the department the Office of Data Privacy.

237 (2) The office shall coordinate with the governing board and the commission to

238 perform the duties in this section.

239 (3) The office shall:

240 (a) create and maintain a strategic data privacy plan to:

241 (i) assist state agencies to implement effective and efficient privacy practices, tools,



242 and systems that:

243 (A) protect the privacy of personal data;

244 (B) comply with laws and regulations specific to the entity, program, or data;

245 (C) empower individuals to protect and control their personal data; and

246 (D) enable information sharing among entities, as allowed by law; and

247 (ii) account for differences in state agency resources, capabilities, populations served,  
248 data types, and maturity levels regarding privacy practices;

249 (b) review statutory provisions related to governmental data privacy and records

250 management to:

251 (i) identify conflicts and gaps in data privacy law;

252 (ii) standardize language; and

253 (iii) consult impacted agencies and the attorney general regarding findings and

254 proposed amendments;

255 (c) work with state agencies to study, research, and identify:

256 (i) additional privacy requirements that are feasible for state agencies;

257 (ii) potential remedies and accountability mechanisms for non-compliance of a state  
258 agency;

259 (iii) ways to expand individual control and rights with respect to personal data held by  
260 state agencies; and

261 (iv) resources needed to develop, implement, and improve privacy programs;

262 (d) monitor high-risk data processing activities within state agencies;

263 (e) receive information from state agencies regarding the sale, sharing, and processing  
264 personal data;

265 (f) coordinate with the Cyber Center to develop an incident response plan for data  
266 breaches affecting governmental entities;

267 (g) coordinate with the state archivist to incorporate data privacy practices into records  
268 management;

269 (h) coordinate with the state archivist to incorporate data privacy training into the  
270 trainings described in Section 63A-12-110; and

271 (i) create a data privacy training program for employees of governmental entities.

272 (4) The data privacy training program described in Subsection (3)(i) shall be made

273 available to all governmental entities, and shall be designed to provide instruction regarding:

274 (a) data privacy best practices, obligations, and responsibilities; and

275 (b) the relationship between privacy, records management, and security.

276 (5) (a) Except as provided in Subsection (5)(b), an employee of a state agency shall

277 complete the data privacy training program described in Subsection (3)(i):

278 (i) within 30 days of beginning employment; and

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

280 (b) An employee of a state agency that does not have access to personal data as part of

281 the employee's work duties is not required to complete the data privacy training program

282 described in Subsection (3)(i).

283 (c) Each state agency is responsible for monitoring completion of data privacy training

284 by the state agency's employees.

285 (6) To the extent that resources permit, the office may provide expertise and assistance

286 to governmental entities for high risk data processing activities.

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

288 **63A-19-302. Chief privacy officer -- Appointment -- Powers -- Reporting.**

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

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

292 (3) The chief privacy officer:

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

294 (b) has administrative authority over the office;

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

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

298 and

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

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

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

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

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

306 **63A-19-401. Duties of governmental entities.**

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

309 (b) (i) If a governmental entity or a contractor described in Subsection (4)(a) is subject  
310 to a more restrictive or specific provision of law than found in this part, the governmental  
311 entity shall comply with the more restrictive or specific provision of law.

312 (ii) For purposes of Subsection (1)(b)(i), Title 63G, Chapter 2, Government Records  
313 Access and Management Act, is a more restrictive and specific provision of law.

314 (c) A governmental entity that is exempt under Section [63G-2-702](#), [63G-2-703](#), or  
315 [63G-2-704](#) from complying with the requirements in Title 63G, Chapter 2, Part 6, Collection of  
316 Information and Accuracy of Records, is exempt from complying with the requirements in  
317 Sections [63A-19-402](#), [63A-19-403](#), and [63A-19-404](#).

318 (2) A governmental entity:

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

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

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

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

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

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

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

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

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

335 (g) may not sell personal data unless expressly required by law;  
336 (h) may not share personal data unless permitted by law;  
337 (i) (i) that is a designated governmental entity, shall annually report to the state privacy  
338 officer:  
339 (A) the types of personal data the designated governmental entity currently shares or  
340 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 designated governmental entity; and  
344 (ii) that is a state agency, shall annually report to the chief privacy officer:  
345 (A) the types of personal data the state agency currently shares or sells;  
346 (B) the basis for sharing or selling the personal data; and  
347 (C) the classes of persons and the governmental entities that receive the personal data  
348 from the state agency; and  
349 (j) (i) except as provided in Subsection (3), an employee of a governmental entity shall  
350 complete a data privacy training program:  
351 (A) within 30 days after beginning employment; and  
352 (B) at least once in each calendar year; and  
353 (k) is responsible for monitoring completion of data privacy training by the  
354 governmental entity's employees.  
355 (3) An employee of a governmental entity that does not have access to personal data of  
356 individuals as part of the employee's work duties is not required to complete a data privacy  
357 training program described in Subsection (2)(j)(i).  
358 (4) (a) A contractor that enters into or renews an agreement with a governmental entity  
359 after May 1, 2024, and processes or has access to personal data as a part of the contractor's  
360 duties under the agreement, is subject to the requirements of this chapter with regard to the  
361 personal data processed or accessed by the contractor to the same extent as required of the  
362 governmental entity.  
363 (b) An agreement under Subsection (4)(a) shall require the contractor to comply with  
364 the requirements of this chapter to the same extent as the governmental entity.  
365 (c) The requirements under Subsections (4)(a) and (b) are in addition to and do not

366 replace any other requirements or liability that may be imposed for the contractor's violation of  
367 other laws protecting privacy rights or government records.

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

369 **63A-19-402. General governmental privacy requirements -- Personal data request**  
370 **notice.**

371 (1) A governmental entity shall provide a personal data request notice to an individual,  
372 or the legal guardian of an individual, from whom the governmental entity requests or collects  
373 personal data.

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

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

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

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

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

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

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

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

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

384 (a) posting the personal data request notice in a prominent place where the  
385 governmental entity collects the personal data;

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

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

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

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

396 (6) The governmental entity may only use personal data furnished by an individual for

397 the purposes identified in the personal data request notice provided to that individual.

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

399 **63A-19-403. Procedure to request amendment or correction of personal data.**

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

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

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

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

409 **63A-19-404. Retention and disposition of personal data.**

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

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

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

416 **63A-19-405. Data breach notification to the Cyber Center and the Office of the**  
417 **Attorney General.**

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

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

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

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

428 (b) include the following information:  
429 (i) the date and time the data breach occurred;  
430 (ii) the date the data breach was discovered;  
431 (iii) a short description of the data breach that occurred;  
432 (iv) the means by which access was gained to the system, computer, or network;  
433 (v) the individual or entity who perpetrated the data breach;  
434 (vi) steps the governmental entity is or has taken to mitigate the impact of the data  
435 breach; and  
436 (vii) any other details requested by the Cyber Center.  
437 (3) For a data breach under Subsection (1)(a), the governmental entity shall provide the  
438 following information to the Cyber Center and the attorney general in addition to the  
439 information required under Subsection (2)(b):  
440 (a) the total number of people affected by the data breach, including the total number  
441 of Utah residents affected; and  
442 (b) the type of personal data involved in the data breach.  
443 (4) If the information required by Subsection (2)(b) is not available within five days of  
444 discovering the breach, the governmental entity shall provide as much of the information  
445 required under Subsection (2)(b) as is available and supplement the notification with additional  
446 information as soon as the information becomes available.  
447 (5) (a) A governmental entity that experiences a data breach affecting fewer than 500  
448 individuals shall create an internal incident report containing the information in Subsection  
449 (2)(b) as soon as practicable and shall provide additional information as the information  
450 becomes available.  
451 (b) A governmental entity shall provide to the Cyber Center:  
452 (i) an internal incident report described in Subsection (5)(a) upon request of the Cyber  
453 Center; and  
454 (ii) an annual report logging all of the governmental entity's data breach incidents  
455 affecting fewer than 500 individuals.  
456 Section 13. Section **63A-19-406** is enacted to read:  
457 **63A-19-406. Data breach notice to individuals affected by data breach.**  
458 (1) A governmental entity shall provide a data breach notice to an individual or legal

459 guardian of an individual affected by the data breach:

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

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

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

463 (2) A governmental entity shall delay providing notification under Subsection (1) at the  
464 request of a law enforcement agency that determines that notification may impede a criminal  
465 investigation, until such time as the law enforcement agency informs the governmental entity  
466 that notification will no longer impede the criminal investigation.

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

468 (a) a description of the data breach;

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

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

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

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

475 (4) Unless the governmental entity reasonably believes that providing notification  
476 would pose a threat to the safety of an individual, or unless an individual has designated to the  
477 governmental entity a preferred method of communication, a governmental entity shall provide  
478 notice by:

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

480 (ii) mail; and

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

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

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

487 (5) A governmental entity shall also provide a data breach notice in a manner that is  
488 reasonably calculated to have the best chance of being received by the affected individual or  
489 the legal guardian of an individual, such as through a press release, posting on appropriate



490 social media accounts, or publishing notice in a newspaper of general circulation when:

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

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

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

495 **Part 5. Data Privacy Ombudsperson**

496 **63A-19-501. Data privacy ombudsperson.**

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

499 (2) The ombudsperson shall:

500 (a) be familiar with the provisions of:

501 (i) this chapter;

502 (ii) Chapter 12, Division of Archives and Records Service and Management of  
503 Government Records; and

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

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

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

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

512 (a) a specific governmental entity; or

513 (b) widespread governmental entity data privacy practices.

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

515 **Part 6. Remedies**

516 **63A-19-601. Enforcement.**

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

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

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

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

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

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

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

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

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

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

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

533 **CHAPTER 24. UTAH PRIVACY COMMISSION**

534 **Part 1. General Provisions**

535 **63C-24-101. Title.**

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

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

539 **63C-24-102. Definitions.**

540 As used in this chapter:

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

543 (2) "Governing board" means the Utah Privacy Governing Board created in Section  
544 [63A-9-201](#).

545 (3) "Governmental entity" means the same as that term is defined in Section  
546 [63G-2-103](#).

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

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

552 ~~[(3)]~~ (4) "Independent entity" means the same as that term is defined in Section  
553 [63E-1-102](#).

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

555 ~~[(4)]~~ (6) ~~[(a)]~~ "Personal data" means ~~[any information relating to an identified or~~  
556 ~~identifiable individual]~~ the same as that term is defined in Section [63A-19-101](#).

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

558 ~~[(5)]~~ (7) (a) "Privacy practice" means the acquisition, use, storage, or disposal of  
559 personal data.

560 (b) "Privacy practice" includes:

561 (i) a technology use related to personal data; and

562 (ii) policies related to the protection, storage, sharing, and retention of personal data.

563 Section 18. Section **63C-24-201** is amended to read:

564 **Part 2. Utah Privacy Commission**

565 **63C-24-201. Utah Privacy Commission created.**

566 (1) There is created the ~~[Personal Privacy Oversight]~~ Utah Privacy Commission.

567 (2) (a) The commission shall be composed of 12 members.

568 (b) The governor shall appoint:

569 (i) one member who, at the time of appointment provides internet technology services  
570 for a county or a municipality;

571 (ii) one member with experience in cybersecurity;

572 (iii) one member representing private industry in technology;

573 (iv) one member representing law enforcement; and

574 (v) one member with experience in data privacy law.

575 (c) The state auditor shall appoint:

576 (i) one member with experience in internet technology services;

577 (ii) one member with experience in cybersecurity;

578 (iii) one member representing private industry in technology;

579 (iv) one member with experience in data privacy law; and

580 (v) one member with experience in civil liberties law or policy and with specific  
581 experience in identifying the disparate impacts of the use of a technology or a policy on  
582 different populations.

- 583 (d) The attorney general shall appoint:
- 584 (i) one member with experience as a prosecutor or appellate attorney and with  
585 experience in data privacy or civil liberties law; and
- 586 (ii) one member representing law enforcement.
- 587 (3) (a) Except as provided in Subsection (3)(b), a member is appointed for a term of  
588 four years.
- 589 (b) The initial appointments of members described in Subsections (2)(b)(i) through  
590 (b)(iii), (2)(c)(iv) through (c)(v), and (2)(d)(ii) shall be for two-year terms.
- 591 (c) When the term of a current member expires, a member shall be reappointed or a  
592 new member shall be appointed in accordance with Subsection (2).
- 593 (4) (a) When a vacancy occurs in the membership for any reason, a replacement shall  
594 be appointed in accordance with Subsection (2) for the unexpired term.
- 595 (b) A member whose term has expired may continue to serve until a replacement is  
596 appointed.
- 597 (5) The commission shall select officers from the commission's members as the  
598 commission finds necessary.
- 599 (6) (a) A majority of the members of the commission is a quorum.
- 600 (b) The action of a majority of a quorum constitutes an action of the commission.
- 601 (7) A member may not receive compensation or benefits for the member's service but  
602 may receive per diem and travel expenses incurred as a member of the commission at the rates  
603 established by the Division of Finance under:
- 604 (a) Sections [63A-3-106](#) and [63A-3-107](#); and
- 605 (b) rules made by the Division of Finance in accordance with Sections [63A-3-106](#) and  
606 [63A-3-107](#).
- 607 (8) A member shall refrain from participating in a review of:
- 608 (a) an entity of which the member is an employee; or
- 609 (b) a technology in which the member has a financial interest.
- 610 (9) The state auditor shall provide staff and support to the commission.
- 611 (10) The commission shall meet up to [~~seven~~] 12 times a year to accomplish the duties  
612 described in Section [63C-24-202](#).
- 613 Section 19. Section **63C-24-202** is amended to read:

614 **63C-24-202. Commission duties.**

615 (1) The commission shall:

616 (a) annually develop a data privacy agenda that identifies for the upcoming year:617 (i) governmental entity privacy practices to be reviewed by the commission;618 (ii) educational and training materials that the commission intends to develop;619 (iii) any other items related to data privacy the commission intends to study; and620 (iv) best practices and guiding principles that the commission plans to develop related  
621 to government privacy practices;622 (b) develop guiding standards and best practices with respect to government privacy  
623 practices;624 ~~[(b)]~~ (c) develop educational and training materials that include information about:625 (i) the privacy implications and civil liberties concerns of the privacy practices of  
626 government entities;627 (ii) best practices for government collection and retention policies regarding personal  
628 data; and629 (iii) best practices for government personal data security standards; ~~[and]~~630 ~~[(c)]~~ (d) review the privacy implications and civil liberties concerns of government  
631 privacy practices[-] ; and632 (e) provide the data privacy agenda to the governing board by May 1 of each year.633 (2) The commission may, in addition to the approved items in the data privacy agenda  
634 prepared under Subsection (1)(a):635 (a) review specific government privacy practices as referred to the commission by the  
636 chief privacy officer described in Section ~~[67-1-17]~~ [63A-19-302](#) or the state privacy officer  
637 described in Section [67-3-13](#); ~~[and]~~638 (b) review a privacy practice not accounted for in the data privacy agenda only upon  
639 referral by the chief privacy officer or the state privacy officer in accordance with Subsection  
640 [63C-24-202\(2\)\(a\)](#);641 (c) review and provide recommendations regarding consent mechanisms used by  
642 governmental entities to collect personal information;643 (d) develop and provide recommendations to the Legislature on how to balance  
644 transparency and public access of public records against an individual's reasonable expectations

645 of privacy and data protection; and

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

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

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

651 (b) the guiding standards and best practices described in Subsection ~~[(1)(a)]~~ (1)(b); and

652 (c) any recommendations for legislation the commission has developed in accordance  
653 with Subsection ~~[(2)(b)]~~ (2)(e).

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

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

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

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

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

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

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

667 **67-3-13. State privacy officer.**

668 (1) As used in this section:

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

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

672 (c) "Governmental entity" means the same as that term is defined in Section  
673 [63G-2-103](#).

674 ~~[(c) (i) "Government entity" means the state, a county, a municipality, a higher~~  
675 ~~education institution, a special district, a special service district, a school district, an~~

676 independent entity, or any other political subdivision of the state or an administrative subunit of  
677 any political subdivision, including a law enforcement entity.]

678 [(ii) "Government entity" includes an agent of an entity described in Subsection  
679 (†)(c)(i).]

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

682 [(ii) "Personal data" includes personally identifying information.]

683 (e) (i) "Privacy practice" means the acquisition, use, storage, or disposal of personal  
684 data.

685 (ii) "Privacy practice" includes:

686 (A) a technology use related to personal data; and

687 (B) policies related to the protection, storage, sharing, and retention of personal data.

688 (f) (i) "State agency" means the following entities that are under the direct supervision  
689 and control of the governor or the lieutenant governor:

690 (A) a department;

691 (B) a commission;

692 (C) a board;

693 (D) a council;

694 (E) an institution;

695 (F) an officer;

696 (G) a corporation;

697 (H) a fund;

698 (I) a division;

699 (J) an office;

700 (K) a committee;

701 (L) an authority;

702 (M) a laboratory;

703 (N) a library;

704 (O) a bureau;

705 (P) a panel;

706 (Q) another administrative unit of the state; or

- 707 (R) an agent of an entity described in Subsections (A) through (Q).
- 708 (ii) "State agency" does not include:
- 709 (A) the legislative branch;
- 710 (B) the judicial branch;
- 711 (C) an executive branch agency within the Office of the Attorney General, the state
- 712 auditor, the state treasurer, or the State Board of Education; or
- 713 (D) an independent entity.
- 714 (2) The state privacy officer shall:
- 715 (a) when completing the duties of this Subsection (2), focus on the privacy practices of
- 716 designated [~~government~~] governmental entities;
- 717 (b) compile information about government privacy practices of designated
- 718 [~~government~~] governmental entities;
- 719 (c) make public and maintain information about government privacy practices on the
- 720 state auditor's website;
- 721 (d) provide designated [~~government~~] governmental entities with educational and
- 722 training materials developed by the [~~Personal Privacy Oversight~~] Utah Privacy Commission
- 723 established in Section [63C-24-201](#) that include the information described in Subsection
- 724 [63C-24-202\(1\)\(b\)](#);
- 725 (e) implement a process to analyze and respond to requests from individuals for the
- 726 state privacy officer to review a designated [~~government~~] governmental entity's privacy
- 727 practice;
- 728 (f) identify annually which designated [~~government~~] governmental entities' privacy
- 729 practices pose the greatest risk to individual privacy and prioritize those privacy practices for
- 730 review;
- 731 (g) review each year, in as timely a manner as possible, the privacy practices that the
- 732 privacy officer identifies under Subsection (2)(e) or (2)(f) as posing the greatest risk to
- 733 individuals' privacy;
- 734 (h) when reviewing a designated [~~government~~] governmental entity's privacy practice
- 735 under Subsection (2)(g), analyze:
- 736 (i) details about the technology or the policy and the technology's or the policy's
- 737 application;



- 738 (ii) information about the type of data being used;
- 739 (iii) information about how the data is obtained, stored, shared, secured, and disposed;
- 740 (iv) information about with which persons the designated [government] governmental
- 741 entity shares the information;
- 742 (v) information about whether an individual can or should be able to opt out of the
- 743 retention and sharing of the individual's data;
- 744 (vi) information about how the designated [government] governmental entity
- 745 de-identifies or anonymizes data;
- 746 (vii) a determination about the existence of alternative technology or improved
- 747 practices to protect privacy; and
- 748 (viii) a finding of whether the designated [government] governmental entity's current
- 749 privacy practice adequately protects individual privacy; and
- 750 (i) after completing a review described in Subsections (2)(g) and (h), determine:
- 751 (i) each designated [government] governmental entity's use of personal data, including
- 752 the designated [government] governmental entity's practices regarding data:
- 753 (A) acquisition;
- 754 (B) storage;
- 755 (C) disposal;
- 756 (D) protection; and
- 757 (E) sharing;
- 758 (ii) the adequacy of the designated [government] governmental entity's practices in
- 759 each of the areas described in Subsection (2)(i)(i); and
- 760 (iii) for each of the areas described in Subsection (2)(i)(i) that the state privacy officer
- 761 determines to require reform, provide recommendations for reform to the designated
- 762 [government] governmental entity and the legislative body charged with regulating the
- 763 designated [government] governmental entity.
- 764 (3) (a) The legislative body charged with regulating a designated [government]
- 765 governmental entity that receives a recommendation described in Subsection (2)(i)(iii) shall
- 766 hold a public hearing on the proposed reforms:
- 767 (i) with a quorum of the legislative body present; and
- 768 (ii) within 90 days after the day on which the legislative body receives the

769 recommendation.

770 (b) (i) The legislative body shall provide notice of the hearing described in Subsection  
771 (3)(a).

772 (ii) Notice of the public hearing and the recommendations to be discussed shall be  
773 posted for the jurisdiction of the designated [~~government~~] governmental entity, as a class A  
774 notice under Section [63G-30-102](#), for at least 30 days before the day on which the legislative  
775 body will hold the public hearing.

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

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

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

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

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

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

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

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

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

792 (5) The state privacy officer shall:

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

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

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

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

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

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

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

804 (iv) reports received from designated governmental entities regarding the sale or  
 805 sharing of personal data provided under Subsection 63A-19-401(2)(f)(i); and

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

808 Section 21. **Repealer.**

809 This bill repeals:

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

811 Section 22. **Effective date.**

812 This bill takes effect on May 1, 2024.

813 Section 23. **Coordinating H.B. 491 with S.B. 98.**

814 If H.B. 491, Data Privacy Amendments, and S.B. 98, Online Data Security and Privacy  
 815 Amendments, both pass and become law, the Legislature intends that, on May 1, 2024:

816 (1) in Subsection 63A-16-1102(4) in S.B. 98, "Section 63A-16-1103" be changed to  
 817 "Section 63A-19-405"; and

818 (2) Section 63A-16-1103 (renumbered from Section 63A-16-511) in S.B. 98 be  
 819 amended to read as follows:

820 "[~~63A-16-511~~] 63A-16-1103. [~~Reporting to the Utah Cyber Center --~~

821 Assistance to governmental entities -- Records.

822 [(1) As used in this section:]

823 [(a) "Governmental entity" means the same as that term is defined in Section  
 824 63G-2-103.]

825 [(b) "Utah Cyber Center" means the Utah Cyber Center created in Section  
 826 63A-16-510.]

827 [(2) A governmental entity shall contact the Utah Cyber Center as soon as practicable  
 828 when the governmental entity becomes aware of a breach of system security.(3)]

829 (1) The [Utah] Cyber Center shall provide [the] a governmental entity with assistance  
 830 in responding to [the] a data breach [of system security] reported under Section 63A-19-405,

831 which may include:

832 (a) conducting all or part of ~~[the]~~ an internal investigation ~~[required under Subsection~~  
833 ~~13-44-202(1)(a)]~~ into the data breach;

834 (b) assisting law enforcement with the law enforcement investigation if needed;

835 (c) determining the scope of the data breach ~~[of system security]~~;

836 (d) assisting the governmental entity in restoring the reasonable integrity of the system;

837 or

838 (e) providing any other assistance in response to the reported data breach ~~[of system~~  
839 ~~security]~~.

840 ~~[(4) (a) A person providing information to the Utah Cyber Center may submit the~~  
841 ~~information required in Section 63G-2-309 to request that the information submitted by the~~  
842 ~~person and information produced by the Utah Cyber Center in the course of the Utah Cyber~~  
843 ~~Center's investigation be classified as a confidential protected record.]~~

844 ~~[(b) Information submitted to the Utah Cyber Center under Subsection 13-44-202(1)(c)~~  
845 ~~regarding a breach of system security may include information regarding the type of breach, the~~  
846 ~~attack vector, attacker, indicators of compromise, and other details of the breach that are~~  
847 ~~requested by the Utah Cyber Center.]~~

848 ~~[(c)]~~ (2) (a) A governmental entity that is required to submit information under Section  
849 ~~[63A-16-511]~~ 63A-19-405 shall provide records to the ~~[Utah]~~ Cyber Center as a shared record  
850 in accordance with Section 63G-2-206.

851 (b) The following information may be deemed confidential and may only be shared as  
852 provided in Section 63G-2-206:

853 (i) the information provided to the Cyber Center by a governmental entity under  
854 Section 63A-19-405; and

855 (ii) information produced by the Cyber Center in response to a report of a data breach  
856 under Subsection (1)."