Utah Code Ann. § 63A-19-301

Current through May 1, 2024 of the 2024 General Session.

Utah Code Annotated > Title 63A Utah Government Operations Code (Chs. 1 — 19) > Chapter 19. Government Data Privacy Act (Pts. 1 — 6) > Part 3. Office of Data Privacy (§ 63A-19-301)

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

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

(2) The office shall coordinate with the governing board and the commission to perform the duties in this section.

(3) The office shall:

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

(i) assist state agencies to implement effective and efficient privacy practices, tools, and systems that:

(A) protect the privacy of personal data;

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

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

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

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

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

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

(ii) standardize language; and

(iii) consult impacted agencies and the attorney general regarding findings and proposed amendments;

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

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

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

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

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

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

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

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

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

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

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

(4) The data privacy training program described in Subsection (3)(i) shall be made available to all governmental entities, and shall be designed to provide instruction regarding:

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

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

(5)

(a) Except as provided in Subsection (5)(b), an employee of a state agency shall complete the data privacy training program described in Subsection (3)(i):

(i) within 30 days of beginning employment; and

(ii) at least once in each calendar year.

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

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

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

History

2024 ch. 417, § 6, effective May 1, 2024.