

**Effective 5/1/2024**

## **Chapter 19 Government Data Privacy Act**

### **Part 1 General Provisions -- State Data Privacy Policy**

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

As used in this chapter:

- (1) "Chief privacy officer" means the individual appointed under Section 63A-19-302.
- (2) "Commission" means the Utah Privacy Commission established in Section 63C-24-102.
- (3) "Cyber Center" means the Utah Cyber Center created in Section 63A-16-1102.
- (4) "Data breach" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by a governmental entity, unless the governmental entity concludes, according to standards established by the Cyber Center, that there is a low probability that personal data has been compromised.
- (5) "Designated governmental entity" means the same as that term is defined in Section 67-3-13.
- (6) "Governing board" means the Utah Privacy Governing Board established in Section 63A-19-201.
- (7) "Governmental entity" means the same as that term is defined in Section 63G-2-103.
- (8) "High risk processing activities" means a governmental entity's processing of personal data that may result in a significant compromise to an individual's privacy interests, based on factors that include:
  - (a) the sensitivity of the personal data processed;
  - (b) the amount of personal data being processed;
  - (c) the individual's ability to consent to the processing of personal data; and
  - (d) risks of unauthorized access or use.
- (9) "Individual" means the same as that term is defined in Section 63G-2-103.
- (10) "Legal guardian" means:
  - (a) the parent of a minor; or
  - (b) an individual appointed by a court to be the guardian of a minor or incapacitated person and given legal authority to make decisions regarding the person or property of the minor or incapacitated person.
- (11) "Office" means the Office of Data Privacy created in Section 63A-19-301.
- (12) "Ombudsperson" means the data privacy ombudsperson appointed under Section 63A-19-501.
- (13) "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.
- (14) "Process" or "processing" means any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.
- (15) "Record" means the same as that term is defined in Section 63G-2-103.
- (16) "Record series" means the same as that term is defined in Section 63G-2-103.
- (17) "Retention schedule" means a governmental entity's schedule for the retention or disposal of records that has been approved by the Records Management Committee pursuant to Section 63A-12-113.

(18)

- (a) "Sell" means an exchange of personal data for monetary consideration by a governmental entity to a third party.
- (b) "Sell" does not include a fee:
  - (i) charged by a governmental entity for access to a record; or
  - (ii) assessed in accordance with an approved fee schedule.

(19)

- (a) "State agency" means the following entities that are under the direct supervision and control of the governor or the lieutenant governor:
  - (i) a department;
  - (ii) a commission;
  - (iii) a board;
  - (iv) a council;
  - (v) an institution;
  - (vi) an officer;
  - (vii) a corporation;
  - (viii) a fund;
  - (ix) a division;
  - (x) an office;
  - (xi) a committee;
  - (xii) an authority;
  - (xiii) a laboratory;
  - (xiv) a library;
  - (xv) a bureau;
  - (xvi) a panel;
  - (xvii) another administrative unit of the state; or
  - (xviii) an agent of an entity described in Subsections (19)(a)(i) through (xvii).
- (b) "State agency" does not include:
  - (i) the legislative branch;
  - (ii) the judicial branch;
  - (iii) an executive branch agency within the Office of the Attorney General, the state auditor, the state treasurer, or the State Board of Education; or
  - (iv) an independent entity.

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

Enacted by Chapter 417, 2024 General Session

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

It is the policy of Utah that:

- (1) an individual has a fundamental interest in and inherent expectation of privacy regarding the personal data that the individual provides to a governmental entity;
- (2) a governmental entity shall act in a manner respecting personal data provided to the governmental entity that is consistent with the interests and expectations described in Subsection (1);
- (3) the state shall encourage innovation to enhance the ability of a governmental entity to:
  - (a) protect the privacy of an individual's personal data;
  - (b) provide clear notice to an individual regarding the governmental entity's processing of the individual's personal data;

- (c) process personal data only for specified, lawful purposes and only process the minimum amount of an individual's personal data necessary to achieve those purposes;
  - (d) implement appropriate consent mechanisms regarding the uses of an individual's personal data;
  - (e) provide an individual with the ability to access, control, and request corrections to the individual's personal data held by a governmental entity;
  - (f) maintain appropriate safeguards to protect the confidentiality, integrity, and availability of personal data;
  - (g) account for compliance with privacy related laws, rules, and regulations that are specific to a particular governmental entity, program, or personal data; and
  - (h) meet a governmental entity's and an individual's business and service needs;
- (4) the state shall promote training and education programs for employees of governmental entities focused on:
- (a) data privacy best practices, obligations, and responsibilities; and
  - (b) the overlapping relationship with privacy, records management, and security; and
- (5) the state shall promote consistent terminology in data privacy requirements across governmental entities.

Enacted by Chapter 417, 2024 General Session

## **Part 2**

### **Utah Privacy Governing Board**

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

- (1) There is created the Utah Privacy Governing Board.
- (2) The governing board shall be composed of five members as follows:
  - (a) the governor, or the governor's designee;
  - (b) the president of the Senate, or the president's designee;
  - (c) the speaker of the House of Representatives, or the speaker's designee;
  - (d) the attorney general, or the attorney general's designee; and
  - (e) the state auditor, or the state auditor's designee.
- (3)
  - (a) A majority of the members of the governing board is a quorum.
  - (b) The action of a majority of a quorum constitutes an action of the governing board.
- (4) The governor, or the governor's designee is chair of the governing board.
- (5) The governing board shall meet at least two times a year.
- (6) The governing board may recommend specific matters to the state auditor under Section 63A-19-601.
- (7) The office shall provide staff and support to the governing board.

Enacted by Chapter 417, 2024 General Session

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

- (1) The governing board shall:
  - (a) recommend changes to the state data privacy policy;

- (b) by July 1 of each year, approve the data privacy agenda items for the commission and make recommendations for additional items for the data privacy agenda;
  - (c) hear issues raised by the ombudsperson regarding existing governmental entity privacy practices;
  - (d) evaluate and recommend the appropriate:
    - (i) structure and placement for the office within state government; and
    - (ii) authority to be granted to the office, including any authority to make rules; and
  - (e) recommend funding mechanisms and strategies for governmental entities to enable compliance with data privacy responsibilities, including:
    - (i) appropriations;
    - (ii) rates;
    - (iii) grants; and
    - (iv) internal service funds.
- (2) In fulfilling the duties under this part, the governing board may receive and request input from:
- (a) governmental entities;
  - (b) elected officials;
  - (c) subject matter experts; and
  - (d) other stakeholders.

Enacted by Chapter 417, 2024 General Session

### **Part 3**

## **Office of Data Privacy**

#### **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.

Enacted by Chapter 417, 2024 General Session

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

- (1) The governor shall, with the advice and consent of the Senate, appoint a chief privacy officer.
- (2) The chief privacy officer is the director of the office.
- (3) The chief privacy officer:
  - (a) shall exercise all powers given to and perform all duties imposed on the office;
  - (b) has administrative authority over the office;
  - (c) may make changes in office personnel and service functions under the chief privacy officer's administrative authority;
  - (d) may authorize a designee to assist with the chief privacy officer's responsibilities; and
  - (e) shall report annually, on or before October 1, to the Judiciary Interim Committee regarding:
    - (i) recommendations for legislation to address data privacy concerns; and
    - (ii) reports received from state agencies regarding the sale or sharing of personal data provided under Subsection 63A-19-401(2)(f)(ii).

Enacted by Chapter 417, 2024 General Session

## Part 4 Duties of Governmental Entities

### 63A-19-401 Duties of governmental entities.

- (1)
  - (a) Except as provided in Subsections (1)(b) and (c), a governmental entity shall comply with the requirements of this part.
  - (b)
    - (i) If a governmental entity or a contractor described in Subsection (4)(a) is subject to a more restrictive or a more specific provision of law than found in this part, the governmental entity or contractor shall comply with the more restrictive or more specific provision of law.
    - (ii) For purposes of Subsection (1)(b)(i), Title 63G, Chapter 2, Government Records Access and Management Act, is a more specific provision of law and shall control over the provisions of this part.
  - (c) A governmental entity that is exempt under Section 63G-2-702, 63G-2-703, or 63G-2-704 from complying with the requirements in Title 63G, Chapter 2, Part 6, Collection of Information and Accuracy of Records, is exempt from complying with the requirements in Sections 63A-19-402, 63A-19-403, and 63A-19-404.
- (2) A governmental entity:
  - (a) shall implement and maintain a privacy program before May 1, 2025, that includes the governmental entity's policies, practices, and procedures for the process of personal data;
  - (b) shall provide notice to an individual or the legal guardian of an individual, if the individual's personal data is affected by a data breach, in accordance with Section 63A-19-406;
  - (c) shall obtain and process only the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose;
  - (d) shall meet the requirements of this part for all processing activities implemented by a governmental entity after May 1, 2024;
  - (e) shall for any processing activity implemented before May 1, 2024, as soon as is reasonably practicable, but no later than January 1, 2027:
    - (i) identify any non-compliant processing activity;
    - (ii) document the non-compliant processing activity; and
    - (iii) prepare a strategy for bringing the non-compliant processing activity into compliance with this part;
  - (f) may not establish, maintain, or use undisclosed or covert surveillance of individuals unless permitted by law;
  - (g) may not sell personal data unless expressly required by law;
  - (h) may not share personal data unless permitted by law;
  - (i)
    - (i) that is a designated governmental entity, shall annually report to the state privacy officer:
      - (A) the types of personal data the designated governmental entity currently shares or sells;
      - (B) the basis for sharing or selling the personal data; and
      - (C) the classes of persons and the governmental entities that receive the personal data from the designated governmental entity; and
    - (ii) that is a state agency, shall annually report to the chief privacy officer:
      - (A) the types of personal data the state agency currently shares or sells;
      - (B) the basis for sharing or selling the personal data; and

- (C) the classes of persons and the governmental entities that receive the personal data from the state agency; and
- (j)
  - (i) except as provided in Subsection (3), an employee of a governmental entity shall complete a data privacy training program:
    - (A) within 30 days after beginning employment; and
    - (B) at least once in each calendar year; and
  - (k) is responsible for monitoring completion of data privacy training by the governmental entity's employees.
- (3) An employee of a governmental entity that does not have access to personal data of individuals as part of the employee's work duties is not required to complete a data privacy training program described in Subsection (2)(j)(i).
- (4)
  - (a) A contractor that enters into or renews an agreement with a governmental entity after May 1, 2024, and processes or has access to personal data as a part of the contractor's duties under the agreement, is subject to the requirements of this chapter with regard to the personal data processed or accessed by the contractor to the same extent as required of the governmental entity.
  - (b) An agreement under Subsection (4)(a) shall require the contractor to comply with the requirements of this chapter with regard to the personal data processed or accessed by the contractor as a part of the contractor's duties under the agreement to the same extent as required of the governmental entity.
  - (c) The requirements under Subsections (4)(a) and (b) are in addition to and do not replace any other requirements or liability that may be imposed for the contractor's violation of other laws protecting privacy rights or government records.

Enacted by Chapter 417, 2024 General Session

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

- (1) A governmental entity shall provide a personal data request notice to an individual, or the legal guardian of an individual, from whom the governmental entity requests or collects personal data.
- (2) The personal data request notice described in Subsection (1) shall include:
  - (a) the reasons the individual is asked to provide the personal data;
  - (b) the intended purposes and uses of the personal data;
  - (c) the consequences for refusing to provide the personal data;
  - (d) the classes of persons and entities that:
    - (i) share the personal data with the governmental entity; or
    - (ii) receive the personal data from the governmental entity on a regular or contractual basis;and
  - (e) the record series in which the personal data is or will be included, if applicable.
- (3) The governmental entity shall provide the personal data request notice by:
  - (a) posting the personal data request notice in a prominent place where the governmental entity collects the personal data;
  - (b) including the personal data request notice as part of any document or form used by the governmental entity to collect the personal data; or

- (c) conspicuously linking to or displaying a QR code linked to an electronic version of the personal data request notice as part of any document or form used by the governmental entity to collect the personal data.
- (4) The personal data request notice required by this section is in addition to, and does not supersede, any other notice requirement otherwise applicable to the governmental entity.
- (5) The governmental entity shall, upon request, provide the personal data request notice to an individual, or the legal guardian of an individual, regarding personal data previously furnished by that individual.
- (6) The governmental entity may only use personal data furnished by an individual for the purposes identified in the personal data request notice provided to that individual.

Enacted by Chapter 417, 2024 General Session

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

- (1) A governmental entity that collects personal data shall provide a procedure by which an individual or legal guardian of an individual may request an amendment or correction of personal data that has been furnished to the governmental entity.
- (2) The procedure by which an individual or legal guardian of an individual may request an amendment or correction shall comply with all applicable laws and regulations to which the personal data at issue and to which the governmental entity is subject.
- (3) The procedure to request an amendment or correction described in this section does not obligate the governmental entity to make the requested amendment or correction.

Enacted by Chapter 417, 2024 General Session

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

- (1) A governmental entity that collects personal data shall retain and dispose of the personal data in accordance with a documented record retention schedule.
- (2) Compliance with Subsection (1) does not exempt a governmental entity from complying with other applicable laws or regulations related to retention or disposition of specific personal data held by that governmental entity.

Enacted by Chapter 417, 2024 General Session

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

- (1)
  - (a) A governmental entity that identifies a data breach affecting 500 or more individuals shall notify the Cyber Center and the attorney general of the data breach.
  - (b) In addition to the notification required by Subsection (1)(a), a governmental entity that identifies the unauthorized access, acquisition, disclosure, loss of access, or destruction of data that compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the governmental entity shall notify the Cyber Center.
- (2) The notification under Subsection (1) shall:
  - (a) be made without unreasonable delay, but no later than five days from the discovery of the data breach; and
  - (b) include the following information:



- (i) the date and time the data breach occurred;
  - (ii) the date the data breach was discovered;
  - (iii) a short description of the data breach that occurred;
  - (iv) the means by which access was gained to the system, computer, or network;
  - (v) the individual or entity who perpetrated the data breach;
  - (vi) steps the governmental entity is or has taken to mitigate the impact of the data breach; and
  - (vii) any other details requested by the Cyber Center.
- (3) For a data breach under Subsection (1)(a), the governmental entity shall provide the following information to the Cyber Center and the attorney general in addition to the information required under Subsection (2)(b):
- (a) the total number of people affected by the data breach, including the total number of Utah residents affected; and
  - (b) the type of personal data involved in the data breach.
- (4) If the information required by Subsection (2)(b) is not available within five days of discovering the breach, the governmental entity shall provide as much of the information required under Subsection (2)(b) as is available and supplement the notification with additional information as soon as the information becomes available.
- (5)
- (a) A governmental entity that experiences a data breach affecting fewer than 500 individuals shall create an internal incident report containing the information in Subsection (2)(b) as soon as practicable and shall provide additional information as the information becomes available.
  - (b) A governmental entity shall provide to the Cyber Center:
    - (i) an internal incident report described in Subsection (5)(a) upon request of the Cyber Center; and
    - (ii) an annual report logging all of the governmental entity's data breach incidents affecting fewer than 500 individuals.

Enacted by Chapter 417, 2024 General Session

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

- (1) A governmental entity shall provide a data breach notice to an individual or legal guardian of an individual affected by the data breach:
- (a) after determining the scope of the data breach;
  - (b) after restoring the reasonable integrity of the affected system, if necessary; and
  - (c) without unreasonable delay except as provided in Subsection (1)(b).
- (2) A governmental entity shall delay providing notification under Subsection (1) at the request of a law enforcement agency that determines that notification may impede a criminal investigation, until such time as the law enforcement agency informs the governmental entity that notification will no longer impede the criminal investigation.
- (3) The data breach notice to an affected individual shall include:
- (a) a description of the data breach;
  - (b) the individual's personal data that was accessed or may have been accessed;
  - (c) steps the governmental entity is taking or has taken to mitigate the impact of the data breach;
  - (d) recommendations to the individual on how to protect themselves from identity theft and other financial losses; and
  - (e) any other language required by the Cyber Center.

- (4) Unless the governmental entity reasonably believes that providing notification would pose a threat to the safety of an individual, or unless an individual has designated to the governmental entity a preferred method of communication, a governmental entity shall provide notice by:
  - (a)
    - (i) email, if reasonably available and allowed by law; or
    - (ii) mail; and
  - (b) one of the following methods, if the individual's contact information is reasonably available and the method is allowed by law:
    - (i) text message with a summary of the data breach notice and instructions for accessing the full notice; or
    - (ii) telephone message with a summary of the data breach notice and instructions for accessing the full data breach notice.
- (5) A governmental entity shall also provide a data breach notice in a manner that is reasonably calculated to have the best chance of being received by the affected individual or the legal guardian of an individual, such as through a press release, posting on appropriate social media accounts, or publishing notice in a newspaper of general circulation when:
  - (a) a data breach affects more than 500 individuals; and
  - (b) a governmental entity is unable to obtain an individual's contact information to provide notice for any method listed in Subsection (4).

Enacted by Chapter 417, 2024 General Session

## **Part 5 Data Privacy Ombudsperson**

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

- (1) The governor shall appoint a data privacy ombudsperson with the advice of the governing board.
- (2) The ombudsperson shall:
  - (a) be familiar with the provisions of:
    - (i) this chapter;
    - (ii) Chapter 12, Division of Archives and Records Service and Management of Government Records; and
    - (iii) Title 63G, Chapter 2, Government Records Access and Management Act; and
  - (b) serve as a resource for an individual who is making or responding to a complaint about a governmental entity's data privacy practice.
- (3) The ombudsperson may, upon request by a governmental entity or individual, mediate data privacy disputes between individuals and governmental entities.
- (4) After consultation with the chief privacy officer or the state privacy officer, the ombudsperson may raise issues and questions before the governing board regarding serious and repeated violations of data privacy from:
  - (a) a specific governmental entity; or
  - (b) widespread governmental entity data privacy practices.

Enacted by Chapter 417, 2024 General Session

## **Part 6 Remedies**

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

- (1) Upon instruction by the board, the state auditor shall:
  - (a) investigate alleged violations of this chapter by a governmental entity;
  - (b) provide notice to the relevant governmental entity of an alleged violation of this chapter; and
  - (c) for a violation that the state auditor substantiates, provide an opportunity for the governmental entity to cure the violation within 30 days.
- (2) If a governmental entity fails to cure a violation as provided in Subsection (1)(c), the state auditor shall report the governmental entity's failure:
  - (a) for a designated governmental entity, to the attorney general for enforcement under Subsection (3); and
  - (b) for a state agency, to the Legislative Management Committee.
- (3) After referral by the state auditor under Subsection (2)(a), the attorney general may file an action in district court to:
  - (a) enjoin a designated governmental entity from violating this chapter; or
  - (b) require a designated governmental entity to comply with this chapter.

Enacted by Chapter 417, 2024 General Session