

DATA GOVERNANCE ORDINANCE TEMPLATE



**Utah Office of
Data Privacy**

DISCLAIMER

This template is provided by the Utah Office of Data Privacy (ODP) as a resource to assist governmental entities. This template is intended to serve as general guidance and a foundational structure only. Governmental entities are responsible for reviewing, customizing, and adapting this template to ensure compliance with applicable laws, regulations, policies, and organizational needs.

The ODP makes no representations or warranties, express or implied, regarding the legal sufficiency or suitability of this template for any specific purpose. By using this template, governmental entities acknowledge and agree that the ODP is not liable for the use or modification of this template. This template is not legal advice and is not a substitute for consultation with legal counsel. Entities should consult with their own legal counsel before finalizing or executing a document based on this template.

1. DATA GOVERNANCE POLICY

- 1.1. (Political Subdivision) hereby finds an individual has a fundamental interest in and inherent expectation of privacy regarding the individual's personal data.ⁱ
- 1.2. (Political Subdivision) shall process personal data in a manner consistent with an individual's privacy interests and expectations.ⁱⁱ
- 1.3. (Political Subdivision) hereby adopts this ordinance to:
 - 1.3.1. protect the privacy of individuals when (Political Subdivision) processes personal data;
 - 1.3.2. ensure personal data is only processed for specified, lawful purposes;
 - 1.3.3. establish appropriate safeguards to protect the confidentiality, integrity, and availability of personal data; and
 - 1.3.4. make and maintain procedures designed to protect the privacy, transparency, legal, and financial rights of individuals directly affected by (Political Subdivision)'s activitiesⁱⁱⁱ.

2. PURPOSE OF DATA GOVERNANCE ORDINANCE

- 2.1. The purpose of this ordinance is to:
 - 2.1.1. codify (Political Subdivision)'s data privacy program; and
 - 2.1.2. ensure (Political Subdivision) complies with all data privacy requirements.

3. AUTHORITY

- 3.1. (Political Subdivision) is authorized under Utah Code § 63G-2-701 to adopt an ordinance regarding its information practices including classification, designation, access, denials, segregation, appeals, management, retention, and amendment of records.
- 3.2. (Political Subdivision) is required by Utah Code § 63A-19-401 to initiate a data privacy program.

4. DEFINITIONS

- 4.1. The definitions used in this ordinance are found in Utah Code §§ 63A-19-101, 63G-2-103, and 63A-12-100.5, except:
 - 4.1.1. "Archives" means the Utah Division of Archives and Records Service created under Utah Code § 63A-12-101;

- 4.1.2. “ARO” means a records officer appointed by a CAO;
- 4.1.3. “CAO” means a chief administrative officer designated by (Political Subdivision);
- 4.1.4. “DARS” means the Division of Archives and Records Service and Management of Government Records statute found at Utah Code § 63A-12-100.5 et seq.;
- 4.1.5. “GDPA” means the Government Data Privacy Act found at Utah Code § 63A-19-101 et seq.;
- 4.1.6. “GRAMA” means the Government Records Access and Management Act found at Utah Code § 63G-2-101 et seq.; and
- 4.1.7. “ODP” means the Utah Office of Data Privacy created in Utah Code § 63A-19-301.

5. DATA GOVERNANCE OFFICIALS

- 5.1. (Political Subdivision) shall designate a CAO or multiple CAOs who shall be responsible for:
 - 5.1.1. fulfilling the duties described in Utah Code § 63A-12-103;
 - 5.1.2. ensuring (Political Subdivision) complies with the requirements in the GDPA, GRAMA, and DARS^{iv}; and
 - 5.1.3. receiving and resolving data privacy complaints^v.
- 5.2. The CAO of (Political Subdivision) shall appoint one or more AROs who will be trained to work with the state archives in the care, maintenance, scheduling, disposal, classification, designation, access, and preservation of records.^{vi}

6. TRAINING

- 6.1. (Political Subdivision) shall ensure all:
 - 6.1.1. AROs complete the online training course established by Archives.^{vii}
 - 6.1.2. employees who have access to personal data or supervise employees who have access to personal data complete a data privacy training program as described in Utah Code § 63A-19-401.2.
- 6.2. (Political Subdivision) shall report the percentage of employees who have completed the data privacy training in the privacy program report.^{viii}

7. RECORDS MANAGEMENT

- 7.1. 7.1. (Political Subdivision) shall:
 - 7.1.1. evaluate all records maintained by (Political Subdivision) and either:
 - 7.1.1.1. create a record series^{ix}; or
 - 7.1.1.2. adopt a records model created by the ODP.

- 7.2. (Political Subdivision) shall establish a procedure by which an individual may request an amendment or correction of:
 - 7.2.1. personal data that has been furnished to (Political Subdivision); or
 - 7.2.2. information concerning an identifiable individual contained in a record maintained by (Political Subdivision).^x
- 7.3. (Political Subdivision) shall develop a form by which an at-risk employee may request their personal data be classified as private.^{xi}

8. ACCESS TO RECORDS

(IF POLITICAL SUBDIVISION HAS ALREADY CREATED OR ADOPTED GRAMA PROCESSES, THEY SHOULD BE REFERENCED OR SUBSTITUTED HERE.)

- 8.1. (Political Subdivision) adopts the following requirements in GRAMA:
 - 8.1.1. Title 63G, Chapter 2, Parts 1, 2, 3, 6, and 8;
 - 8.1.2. Utah Code § 63G-2-400.5;
 - 8.1.3. Utah Code § 63G-2-401, except the CAO shall notify the requester an appeal of the CAO's decision may only be made to the local appeals board or the district court;
 - 8.1.4. Utah Code § 63G-2-402, except an appeal of the CAO's decision may only be made to the local appeals board or the district court;
 - 8.1.5. Utah Code § 63G-2-404;
 - 8.1.6. Utah Code § 63G-2-405;
 - 8.1.7. Utah Code § 63G-2-406; and
 - 8.1.8. Utah Code § 63G-2-701.

9. REQUIREMENTS FOR PROCESSING PERSONAL DATA

- 9.1. (Political Subdivision) shall only obtain and process the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose.^{xii}
- 9.2. (Political Subdivision) shall ensure compliance with all privacy requirements for any new processing activities implemented by (Political Subdivision).^{xiii}
- 9.3. For any non-compliant processing activities previously implemented, (Political Subdivision) shall:
 - 9.3.1. identify the non-compliant processing activities;
 - 9.3.2. prepare a strategy for bringing the non-compliant processing activities into compliance; and
 - 9.3.3. include this information in the privacy program report.^{xiv}

10. LIMITATIONS ON PROCESSING PERSONAL DATA

- 10.1. (Political Subdivision) may only:
 - 10.1.1. establish, maintain, or use undisclosed or covert surveillance of individuals as permitted by law^{xv};
 - 10.1.2. share personal data if permitted by law^{xvi}; or
 - 10.1.3. sell personal data if expressly required by law^{xvii}.
- 10.2. Personal data may only be used by (Political Subdivision) for the purposes identified in the privacy notice provided to the individual.^{xviii}
- 10.3. User data may only be collected by (Political Subdivision) if all website privacy notice requirements have been met.^{xix}

11. TRANSPARENCY

- 11.1. (Political Subdivision) shall provide a privacy notice if (Political Subdivision) requests or collects personal data from an individual.^{xx}
 - 11.1.1. If the personal data collected is a public record, the privacy notice shall state “the individual's personal data may be available to the public as provided by Section 63G-2-201”.^{xxi}
 - 11.1.2. If the personal data is not classified as a public record the privacy notice shall describe:
 - 11.1.2.1. all intended purposes and uses of the personal data;
 - 11.1.2.2. the consequences for refusing to provide the personal data;
 - 11.1.2.3. the classes of persons and governmental entities:
 - 11.1.2.3.1. with whom (Political Subdivision) shares personal data; and
 - 11.1.2.3.2. to whom (Political Subdivision) sells personal data; and
 - 11.1.2.4. the record series in which the personal data is included.^{xxii}
 - 11.1.3. Upon request, (Political Subdivision) shall provide an individual with a privacy notice regarding personal data the individual previously provided to (Political Subdivision).^{xxiii}
- 11.2. Political Subdivision shall prominently post a website privacy notice on the homepage of (Political Subdivision)’s website.^{xxiv}
 - 11.2.1. The website privacy notice shall include:
 - 11.2.1.1. the identity of (Political Subdivision);
 - 11.2.1.2. how to contact (Political Subdivision);
 - 11.2.1.3. the method by which an individual may:
 - 11.2.1.3.1. seek access to the individual's personal data or user data;

- 11.2.1.3.2. request to correct or amend the individual's personal data or user data;
and
- 11.2.1.3.3. how to contact the Data Privacy Ombuds; and
- 11.2.1.4. how an at-risk employee may request that the at-risk employee's personal information be classified as a private record.^{xxv}
- 11.2.2. If (Political Subdivision)'s website uses tracking technology to collect user data, the website privacy notice shall also include:
 - 11.2.2.1. any website tracking technology used to collect user data on the government website;
 - 11.2.2.2. what user data is collected by (Political Subdivision)'s website;
 - 11.2.2.3. all intended purposes and uses of the user data;
 - 11.2.2.4. the classes of persons and governmental entities:
 - 11.2.2.4.1. with whom (Political Subdivision) shares user data; or
 - 11.2.2.4.2. to whom (Political Subdivision) sells personal data; or
 - 11.2.2.4.3. from whom (Political Subdivision) purchases user data; and
 - 11.2.2.5. the record series in which the user data is included.^{xxvi}

12. SECURITY

- 12.1. (Political Subdivision) shall ensure any contracts (Political Subdivision) enters into with a contractor contains language which requires the contractor to comply with the same security and data privacy requirements as (Political Subdivision).^{xxvii}
- 12.2. (Political Subdivision) shall retain and dispose of records according to the record series created or adopted by (Political Subdivision).^{xxviii}
- 12.3. (Political Subdivision) shall have an incident response plan in place that includes procedures for providing notice of a data breach or security incident to the Attorney General's Office and the Utah Cyber Center.^{xxix}
- 12.4. If (Political Subdivision) identifies the unauthorized access, unauthorized acquisition, unauthorized disclosure, loss of access, or unauthorized destruction of personal data that is used or is reasonably likely to be used to commit theft, fraud, or other criminal acts, (Political Subdivision) shall provide notification of the breach to:
 - 12.4.1. each individual whose personal data is involved in the breach; and
 - 12.4.2. the attorney general.^{xxx}
- 12.5. (Political Subdivision) or a contractor of (Political Subdivision) shall cause a data breach notice to be sent to an individual affected by a data breach.^{xxxi}
- 12.6. If the personal data involved in the data breach is a public record (Political Subdivision) shall prominently post notice of the data breach on the homepage of (Political Subdivision)'s government website.^{xxxii}

13. COMPLIANCE

- 13.1. Each year by December 31st, (Political Subdivision) shall prepare a privacy program report as described in Utah Code § 63A-19-401.3 and share the report with the ODP.

-
- ⁱ Utah Code § 63A-19-102(1).
 - ⁱⁱ Utah Code § 63A-19-102(2).
 - ⁱⁱⁱ Utah Code § 63A-12-103(4).
 - ^{iv} Utah Code § 63A-12-103(9).
 - ^v Utah Code § 63A-19-502.
 - ^{vi} Utah Code § 63A-12-103(2).
 - ^{vii} Utah Code §§ 63A-12-103(3) and 63A-2-110.
 - ^{viii} Utah Code § 63A-19-401.2(4).
 - ^{ix} Utah Code § 63G-2-307.
 - ^x Utah Code § 63A-19-403(1) and 63G-2-603.
 - ^{xi} Utah Code § 63A-19-408.
 - ^{xii} Utah Code § 63A-19-401(2)(a)(ii).
 - ^{xiii} Utah Code § 63A-19-401(2)(a)(iii).
 - ^{xiv} Utah Code § 63A-19-401(2)(a)(iv).
 - ^{xv} Utah Code § 63A-19-401(3)(a).
 - ^{xvi} Utah Code § 63A-19-401(3)(c).
 - ^{xvii} Utah Code § 63A-19-401(3)(b).
 - ^{xviii} Utah Code § 63A-19-402(7).
 - ^{xix} Utah Code § 63A-19-402.5(4).
 - ^{xx} Utah Code § 63A-19-402(1).
 - ^{xxi} Utah Code § 63A-19-402(2)(a).
 - ^{xxii} Utah Code § 63A-19-402(2)(b).
 - ^{xxiii} Utah Code § 63A-19-402(6).
 - ^{xxiv} Utah Code § 63A-19-402.5.
 - ^{xxv} Utah Code § 63A-19-402.5(1).
 - ^{xxvi} Utah Code § 63A-19-402.5(2).
 - ^{xxvii} Utah Code § 63A-19-401.4.
 - ^{xxviii} Utah Code § 63A-19-404.
 - ^{xxix} Utah Code § 63A-19-405.
 - ^{xxx} Utah Code § 63A-19-405(1)(c).
 - ^{xxxi} Utah Code § 63A-19-406(1)(a).
 - ^{xxxii} Utah Code § 63A-19-406(1)(b).