OFFICE OF THE
STATE AUDITOR

This document is for educational purposes only and needs to be customized further. Reach out to the State Privacy Officer at wphillips@utah.gov before implementation.

Privacy Policy Simple Template

(this document is related to the Privacy Program requirement under The Utah Government Data Privacy Act)

Definitions:

Personal Data: information that is linked or can be reasonably linked to an identified individual or an identifiable individual.

Processing: 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.

Sale of data: exchange of personal data for monetary consideration by a governmental entity to a third party.

Introduction

At [Your Organization Name], we prioritize privacy and data security. This Privacy Policy outlines our commitment to safeguarding personal data in compliance with applicable laws and regulations as well as the Utah Fundamental Privacy Principles.

General Rules:

Each employee, volunteer, contractor, or other person related to our organization who has access to personal data is obligated to follow this policy and adhere to the Utah Fundamental Privacy Principles.

Each person with access to personal data is obligated, to the best of their ability, to only work with the minimal amount of data needed, and to protect the data they have been entrusted with, to ensure data is not inappropriately shared or exposed and to prevent over-collection and over-retention.

Each person with access to personal data is trained periodically by us, both at the start of their work with us, and on at least an annual basis thereafter.

Each person with access to personal data is responsible for reporting personal data incidents or other adverse events they observe to their manager/dedicated IT or Privacy Officer without delay.

Each person with access to personal data is only allowed to access data to which they have a legitimate need to know and report to their manager/dedicated IT or Privacy Officer if they believe they have wider access than needed.

Persons with access to personal data are not permitted to engage in sale of personal data unless it is required by law. Fees (based on an approved schedule) charged for access to records are not considered sale of personal data.

Data Collection and Usage

- We collect and process personal data only for specific, lawful purposes and follow the Utah Fundamental Principles for Data processing. For an overview of the principles see Attachment A. For data inventory information see Attachment B
- Personal data is used solely for the purpose it was collected, unless consent or legal obligations require otherwise.
- We do not sell or otherwise monetize your data.
- Personal data is deleted once its retention period expires and the data is no longer needed.

Data Access and Sharing

- Access to personal data is restricted to authorized personnel. You can find more details at (refer to Access Policy).
- We share personal data with third parties only when necessary and in compliance with data protection regulations and under contracts that include necessary data requirements. For a sample of our basic privacy clauses see Attachment C.

Data Retention

- We retain personal data only as long as needed for its intended purpose or as legally required.
- (refer to retention schedules/ records retention policy and Records Officer and the process employees should follow to comply.)

Data Security

- We employ security measures to protect personal data, including encryption and access controls.
- (describe measures)
-

Data Subject Rights

- Individuals have rights under respective laws, such as GRAMA, that may include access, rectification, erasure, data portability, and objection to data processing rights. For more detail on these rights contact your Privacy/Records Management officer at:

Data Breach Response

- We have procedures to detect, report, and respond to data breaches promptly, including notifying affected individuals and authorities.
- (describe procedures high level and refer to more detailed document)

Privacy Officer

- Privacy Officer oversees data protection and privacy compliance, monitors the privacy program, responses to data privacy complaints and serves as a point of contact for an individual's privacy rights. Our Privacy Officer can be contacted at: (Provide contact details)

Information Security Officer:

- An Information Security Officer (ISO) oversees the protection of an organization's computers systems and data from cyber threats. They implement security measures, monitor systems for breaches and ensure compliance with security standards and regulations. Our Security Officer can be contacted at: (Provide contact details)

Training and Awareness

- Employees and contractors receive training on data protection responsibilities.
- (describe frequency and method on a high level. Recommended is A) within 60 days of new role as well as B) at least once a year. Security and privacy training can be done in one session or module but BOTH have to be addressed, not just cyber security)

Compliance Monitoring

- We regularly review and update privacy policies to ensure compliance with respective laws (enter frequency, recommend is once a year)
- For an example of our monitoring metrics see attachment D

Questions and Contact Information

For questions or concerns, contact us at [Contact Information].

Attachment A

Utah Fundamental Privacy Principles

1. Individual Participation

   Give people control of their information when possible.

2. Lawful, Fair, and Responsible use

   Collection, use and disclosure is:

   - Based on legal authority;
   - Not deceptive
   - Not discriminatory or harmful; and
   - Relevant and readably necessary for legitimate purposes.

3. Data Minimization

   The minimum amount of information is collected, used, or disclosed to accomplish the stated purpose for collecting the information.

4. Transparency and Accountability

   Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances. Accountability means being responsible and answerable for following data privacy laws and principles.

5. Security

   Appropriate administrative, technical and physical security practices to protect the confidentiality, integrity, availability and control of personal information.

6. Due Diligence

   Taking reasonable steps and exercising care before and after entering into an agreement or arrangement with a third party that includes sharing personal information.

Attachment B

Personal data notice:

We collect the following data elements for the following purposes and share them with the following classes of people and entities:

Attachment C

Sample Privacy Clauses for vendors.

This can be used as a starting point:

https://auditor.utah.gov/wp-content/uploads/sites/6/2023/08/Privacy-Contract-Clauses-8-29-23.pdf

Attachment D

Overview of recommended monitoring metrics under the Privacy Program:

1. Privacy Policy and Notices

A government entity has updated Privacy Policy Statements and Privacy Notices (at data collection), which undergo yearly updates and are available to the public.

Metrics to measure:

1. Designated governmental entity has a properly published privacy policy that the employees or other persons with access to organizations data are required to adhere to Yes/no

2. Designated governmental entity has a privacy policy statement on their website - Yes/No

3. Such statement has been reviewed/updated within the last 12 months - Yes/No

4. Such statement complies with legal requirements outlined in code - Yes/No

5. Designated government entity embeds privacy notices (Data Processing Request Notices) at entry points of data collection - Yes/No

6. Such notices are periodically (at least annually) reviewed for accuracy - Yes/No

2. Regular Health Checks

A government entity conducts regular checks to assess compliance with privacy policies and procedures. Recommended frequency is annually. Audits or health-checks can identify areas of non-compliance and help designated government entities take corrective action to ensure that privacy policies are being followed.

Metrics to measure:

1. Health-check conducted within last 24 months - Yes/No,

2. Outcome shows improvement since the last check was performed – Yes/No / N/A

3. Incident Tracking

A government entity tracks privacy incidents and data breaches. By tracking incidents, designated government entities can identify patterns and trends that may indicate weaknesses in privacy policies and procedures.

Metrics to measure:

1. Incident tracking is being done - Yes/No

2. Trends of reported incidents show rise of awareness (reported numbers are not zero in more than one measured consecutive period) - Yes/No

3. Root-cause analysis is being performed - Yes/No

4. Ratio of incidents vs breaches is bigger than 1:1 - Yes/No

5. Lessons learned are implemented - Yes/No

6. Annual report provided to the Utah Cyber Center Yes/No

7. Tracking of breaches reportable to the Utah Cyber Center and the Attorney General's Office is conducted on annual basis: Yes-No

4. Privacy Training

A government entity provides privacy training to employees to ensure that they understand the importance of privacy policies and know how to follow them. Ongoing training helps employees stay up-to-date on changes to privacy policies and procedures.

Metrics to measure:

1. Mandatory privacy specific training for is assigned to all new hires - Yes/NO
2. Mandatory training extends to vendors and volunteers - Yes/No
3. Annual mandatory training that is privacy specific is provided to all employees - Yes/No
4. Records of completion/attendance of all trainings is kept - Yes/No
5. Training modules get updated annually to reflect new changes in best practices and laws Yes/No
6. Additional training (especially role specific or law specific) is provided on regular basis Yes/No

5. Privacy Impact Assessments (PIAs)

A government entity conducts PIAs to identify potential privacy risks associated with new projects or initiatives. PIAs can help designated government entities design privacy safeguards that are built into new systems or processes from the outset.

Metrics to measure:

1. Number of PIAs conducted is >0 for measured period - Yes/No
2. PIA conducted for each project involving a large amount (over 100 000 data elements) of data - Yes/No.
3. Conducted PIAs records kept for at least 3 years from the date the PIA was conducted Yes/No

6. Internal Reporting

A government entity encourages employees to report any privacy incidents or concerns to the designated government entity's representative or SPO. This can help entity identify potential areas of non-compliance and take corrective action.

Metrics to measure:

1. Designated government entity has a dedicated Privacy/ Records Management Officer- Yes/No
2. Such officer has undergone specific training /obtained certification for their role - Yes/No
3. Designated government entity has several avenues dedicated to incident reporting - Yes/No

7. Privacy Rights

A government entity is able to respond to data subject requests and furnish their rights, such as right to access, correct or delete their personal data. Due responses help build trust in the government.

Metrics to measure:

1. Individual Request Response time measured - Yes/No
2. Majority of Data Subject Request Response time within a legislated time frame - Yes/No
3. Response time improved since last period metrics were collected for - Yes/No

8. Privacy Complaints

A government entity tracks privacy complaints, analyzes root cause and embeds appropriate safeguards based on findings.

Metrics to measure:

1. Designated government entity tracks number of complaints per year - Yes/No
2. Overall number of substantiated complaints is smaller than last measured period or corresponds with extra activities to raise awareness about complaint process - Yes/No
3. All complaints have been resolved and complainant informed on results - Yes/No
4. Time to resolve complaints is tracked - Yes/No

9. Records Retention Schedules

A government entity periodically reviews their adherence to respective records retention schedules, practices clean desk exercise and has an updated policy on records management and data classification.

Metrics to measure:

1. entity conducts an annual review of obsolete records - Yes/No
2. entity undertakes steps to establish record classification standard - Yes/No
3. entity includes records management in yearly mandatory training - Yes/No
4. entity submits necessary documents to the State Archives per respective code section - Yes/No.
5. Records Officer certification is in compliance at time of check – Yes/No

10. Third Party management

A government entity adequately manages its vendors that may have access to the entity's data, stores underlying documents properly and monitors compliance.

Metrics to measure:

1. Repository of contracts exists - Yes/No

2. Contracts include appropriate privacy clauses, vetted by legal counsel - Yes/No

3. At the end of the relationship the vendor is required to produce certificate of destruction of data - Yes/No

4. The owner of the relationship has been clearly assigned - Yes/No.

5. Third party with access to data are periodically mapped and the results of such mapping is annually reported to the State Privacy Officer.