Last Modified: January 21, 2025

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

Basic Privacy Impact Assessment (PIA)

Name of the person filling out the PIA / providing information on behalf of the governmental entity
Project Owner:
Entity:
Date of PIA:
Privacy Officer /Assessor name:

Name of the project/ record processing (and brief description):

1. **Primary Group of individuals affected by the data collection (check all that apply)**

Employees	Tenants	Constituents	Minors	Customers
Contractors	3rd Parties	Property owners	Students	Volunteers

Other / secondary groups (specify):

2. **Number of Affected Individuals:**
   1-100
   101-1,000
   1,001-10,000
   10,001-100,000
   100,001-500,000
   Above 500,000

Check all data collected for this project/purpose:

Identifying Numbers

Social Security	State ID	Alien Registration	Taxpayer ID	Financial Account
Driver's License	Employee ID	Banking ID	Passport Number	Patient ID File
Case ID	Credit Card	Complaint ID	Tenant ID	Customer ID

Other identifying data (specify):

General Personal Data

Name	Date of Birth	Place of Birth	Maiden Name	Religion
Age	Home Address	Mailing Address	Email Address	Telephone #
Military Service	Financial Info	Gender	Marital Status	License Plate #
Education Level	Schools Attended	Citizenship	Former Legal Name	Social Media Name

Other general personal data (specify):

Work-Related Data

Occupation	Title	Telephone #	Salary	Org. Chart Level
Email Address	Work History	Work Address	References	Performance Rank

Other work-related data (specify):

Distinguishing Features / Biometrics

Fingerprints	Photos	DNA Profiles	Palm Prints	Scars
Marks	Tattoos	Retina/Iris Scans	Voice Recording	Signatures
Vascular Scan	Dental Profile	Gait Analysis	Behavior Metrics	Video

Other distinguishing features/biometrics (specify):

Sensitive Data

Health Condition	Disability Records	Sexual Orientation	Race/ Ethnicity	Mental Health
Political Affiliation	Voting Records	Criminal Records	Welfare Records	Financial History

Other sensitive data (specify):

System Admin / Audit Data

User ID	Login/ Passwords	Time of Access	ID Files Accessed	IP Address
Queries Run	Contents of Files	MAC Address	IMEI/ UDID #	Cookies

Other system/audit data (specify):

Other information (specify):

3. **Source of the data** *(how was the data obtained):*
   Describe: *(include primary tools and 3rd parties involved in the data collection)*

4. **Data Map/Flow:** *Attach a diagram showing how data moves through the system, from collection to disposal, highlighting any points where data is transferred between entities (internal or external). Indicate key data transfer mechanisms (e.g., APIs, file transfers) and control measures in place (e.g., encryption, secure channels). In addition, you may write out the data flow in this area.*

5. **Purpose for which data is collected:** *Describe the purpose for the collection and how the collected data is to be used to achieve the primary purpose, indicate if only minimal extent of data is in scope. If data minimization is not observed, please justify the inclusion of any additional data.*

6. **Access rights:** *List groups/roles that have access to the data throughout their lifecycle, including where the data is going to be stored and how access to it is managed and monitored and if data or workers from other states/nations are going to be used as part of this project.*

7. **Data sharing and disclosures:** *Describe data sharing and its underlying mechanisms and legal basis. Include internal as well as external disclosures. Include whether legal and cybersecurity departments have been involved to review the proposed sharing mechanisms and if any cross-border transfers are planned.* ***List/Attach underlying contracts with 3rd parties****.*

8. **Notice and consent**
Was notice on data collection provided to the individuals before data collection? Y/N
Was the data provided based on consent? Y/N
Can the consent be easily revoked? Y/N
    - *How is consent recorded, managed, and stored?*
    - *What is the process for withdrawing consent?*

    Attach notice language to the report.

9. **Describe measures** *(including information security) taken to mitigate the risk of unauthorized disclosure.*
For each measure, specify whether it is ***Preventative*** *(designed to stop risks before they occur, such as encryption, strong passwords, and access controls),* ***Detective*** *(aimed at identifying and detecting potential risks, such as security monitoring, audit logs, and intrusion detection systems), or* ***Corrective*** *(focused on resolving issues and minimizing impact after an incident, such as incident response plans, data recovery procedures, and breach-related user training)*

    - **Administrative safeguards** (policies, standards, contracts, training, incident response plan...):

- **Physical safeguards** (cabinets, locks, secure doors, CCTV, shredders...)

- **Technical safeguards** (encryption, passwords, multi-factor authentication (MFA), firewalls, testing...)

10. **Retention period:** *Indicate how long the information will be retained to accomplish the primary purpose, any legal or regulatory requirements for retention, how the data will be disposed of at the end of the retention period, and whether a data disposal process is in place. Include the data destruction method and whether a data destruction log is used.*

11. **Decision making:** *Are decisions directly affecting the individual's privacy rights carried out in connection with this processing? Y/N*
    If yes, will such decisions be automated. Y/N
    - *If yes, what criteria are used in the automated decision-making process?*

    - *Can a human review or override these automated decisions? Y/N*

12. **Potential threats**: *Describe any potential threats to privacy as a result of the use of the information, and mirroring controls that have been put into place to ensure that the information is handled, retained, and disposed of appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information based on the retention schedule…)*

13. **Data breach and notification:** *In the event of a data breach, describe the steps that will be taken to mitigate the impact on affected individuals and the timeline for notification.*

14. **Ethical use of data:** *Was the above-described use of data evaluated for compliance with ethical standards, including the use of data within AI tools or other novel technologies? Y/N*
    If so, explain:

List of documents attached to this PIA (include all documents referred to in this PIA):

The following section is to be filled out by the person/s evaluating the privacy impact:

PIA evaluation was performed by:
Date of PIA evaluation:

Over-collection? Y/N

Over-retention? Y/N

Suitable legal bases identified? Y/N

Adequate data security methods applied? Y/N

Access rights adequately managed? Y/N

Notice/Consent mechanism implemented? Y/N

High Exposure? Y/N

High Risk Activity? Y/N

Results:

Inherent privacy risk unmitigated
Inherent privacy risk mitigated inadequately
Residual privacy risk inadequately high
Residual privacy risk adequately controlled

Recommendations for adjustments:

Last Modified: January 21, 2025

PIA – APPENDIX 1

REQUEST FOR NEW USE / DISCLOSURE OF DATA

(To be filled out if/when the scope of the project changes)

Requestor:
Requesting entity:
Date:

Describe the request including its purpose and records in scope. Highlight if new data elements are going to be part of the project.

1. **Would new individuals/groups of individuals have access to the data?** *Y/N*
   - *If yes, what individuals/groups of individuals?*
   - *If yes, what data elements would be shared? List all.*

2. **Have the individuals whose data is being processed consented** *to the new use of their data? Y/N*
   - *If yes, was the consent given in writing and was it a stand-alone consent?*
   - *If not, is there a legal basis allowing for such disclosure? If yes,* ***please specify relevant sections of the law****:*

3. **How would the data be stored and transmitted?** *(describe the method including its security)*

4. **If new recipients are involved, are they legally or contractually required to keep the data confidential, only use it for primary purpose, follow prompt breach notifications** *and securely dispose of it once their purpose has been achieved? Y/N*

5. **Can the same purpose be achieved if data is aggregated or anonymized?** *Y/N*
   - *If yes, what aggregation or anonymization standard will be applied?*
   - *If no, can partial data fulfill the purpose of the request?*
   - *If no, in case of unauthorized access to the full dataset, what is the likelihood of the disclosure causing harm to the individuals?*

Pick one:

Very unlikely
Unlikely,
Likely
Very Unlikely or
Unknown

Examples of harm: public embarrassment, financial loss, reputational loss, identity theft.

6. **Evaluation:**

Is sensitive or biometric data in scope? Y/N	(0/1)
Was notice and consent for this use/disclosure provided? Y/N	(0/1)
Is harm likely if data abused? Y/N	(0/1)
Is harm very likely? Y/N	(0/2)
Is such disclosure reasonably expected? Y/N	(0/1)
Are reasonable security controls applied? Y/N	(0/1)
Is there a statement in code allowing such disclosure? Y/N	(0/1)
Is the data partial, aggregated or anonymized? Y/N	(0/1)
Has legal and cyber security reviewed this proposed transaction? Y/N	(0/1)

7. **Score: 0-10**

0 - 1 – Use/disclosure can be made
2 and higher – Privacy Officer should be consulted before proceeding further.