STATE OF UTAH

Office of Data Privacy

DRAFT Privacy Impact Assessment

Version 1.0

THE GREAT SEAL OF THE STATE OF UTAH 1896

Utah Office of Data Privacy

Privacy Impact Assessment

(IT Systems and On-line Applications)

Introduction

This Privacy Impact Assessment (PIA) from the Office of Data Privacy (ODP) and the Division of Technology Services (DTS) is required to be completed by **all state agencies** for all IT Systems and On-Line Applications that may process personal information prior to processing personal information in the IT System or On-Line Application. (Utah Administrative Code R895-8-8, Utah Code § 63A-12-103(4) and DTS Information Security Policy (Internal) 5000-0002).

This PIA is also designed as a guide for **governmental entities** to identify, assess and mitigate privacy risks to the **Individuals** for which they process **personal information**. Once privacy risks are identified, the governmental entity is directed to identify specific actions (safeguards) the organization will take to lower the risks to **Individuals** that have been identified.

Instructions

Before you get started, set up a central place to store all of your PIAs since you have an obligation to keep them for four years (***See* R895-8-8**) as accountability documentation to prove your compliance with the Privacy Practice to conduct PIAs. Your completed PIAs may be managed as part of **Record Series 31140** and **GRS 1713** If your entity does not have a specific record series created to manage them. The Retention Schedule aligns with the requirement to keep the PIAs for four years as outlined above and/or as long as the processing occurs.

F**amiliarize yourself with the PIA**:. Each section of the PIA is based on generally applicable governmental entity legal requirements. Most sections and questions include references and citations. These should provide you with the materials information you need to research and answer your questions from primary sources. The Office of Data Privacy is available to answer questions and provide training on completing the PIA. You can contact us directly at: officeofdataprivacy@utah.gov, and our website is located here: https://privacy.utah.gov/.

—---

General Information

Name of **Governmental Entity**: ______________________________

Name of the Chief Administrative Officer (Utah Code § 63A-12-103):______________

Name of **Individual** Responsible for PIA (Utah Code § 63A-12 -103(4) and Utah Admin Code R895-8. DTS Information Security Policy 5000-0002): ______________________

Insert URL to Your Organization's Data Inventory (Utah Code §§ 63A-12-103, 63A-12-104, 63A-19-401, and DTS Information Security Policy 5000-0002): ______________________

Insert URL to Your Organization's **IT System or Online Application** Inventory (Division of Technology Services (DTS) Information Security Policy 5000-0002, section 2.4.2.1 and Utah Code § 63A-19-401): ______________________

Insert URL to Your Organization's Records Series Inventory (Utah Code §§ 63G-2-103 and 307): ___

List the statute(s) that authorize(s) the organization to process the personal information listed in your organization's Data Inventory (**Legal Authority)**: ______________________

Date PIA Completed: ______________________

Date PIA Approved: ______________________

Name and Role of Individual PIA Approver: ______________________

Date PIA Completely Operationalized with Safeguards listed below: ______________________

Name and Role of Individual Operationalization Approver: ______________________

Insert URL to this Completed and Official Document: ______________________

Scope of Governmental Entity Reach

Brief description of the product or services your organization provides: ______________________

Number of Utah residents served annually: ______________________

Number of Governmental Entity website visitors annually: ______________________

Number of employees: ______________________

Number of contingent workers: ______________________

Your organization's total annual budget:______________________

Screening Questions

1. Is this a new **IT System** or **On-Line Application**?

   □ Yes

   □ No

   If yes, describe and proceed to question 3:

   If not, proceed to question 2.

2. Are you modifying an existing **IT System** or **On-Line Application**?

□ Yes

□ No

If yes, describe and proceed to question 3:

If not, please look for any previous PIAs or a relevant PIA to be sure. Proceed to question 3.

3. Will you be **Processing Personal Information,** whether it is **De-identified** or not?

□ Yes

□ No

If yes, proceed to question 4.

If not, there is no need to conduct a PIA. Please assign a record series to this document (**Record Series 31140**) and store this assessment in the appropriate file. STOP here.

4. What is the relationship between your organization and the **Data Subject** (select all that apply)?

□ Resident

□ Website visitor

□ Employee

□ Contingent Worker (3rd Party)

□ Independent Contractor (3rd Party)

□ Strategic Partner (3rd Party)

□ Other (please describe):

5. Please select the approximate number of **Data Subjects** impacted.

□ < 500 Individuals

□ 501-<1000 Individuals

□ 1000 - <10,000 Individuals

□ 10,000 - <50,000 Individuals

□ 50,000 - <100,000 Individuals

□ 100,000 - <500,000 Individuals (large scale processing)

□ 500,000 - <1 million Individuals (large scale processing)

□ 1 million Individuals or more (large scale processing)

6. Please select the approximate age range(s) of the **Data Subjects** impacted (select all that apply).

□ < 13 years of age

□ 13 - < 18 years of age

□ 18 - < 65 years of age

□ 65 years of age or older

7. How will the **Personal Information** be collected (select all that apply)?

□ Directly from the **Data Subject**

□ Indirectly from a public source

□ Indirectly from another government entity

□ Indirectly from a non-government entity (3rd party)

□ Other (please describe):

8. Are you collecting new **Personal Information**?

□ Yes

□ No

□ Not Sure (please explain):

9. Are you collecting **Sensitive Personal Information** or **Personal Information** from incapacitated Individuals?

□ Yes

□ No

□ Not Sure (please explain):

10. Does your **IT System or On-Line Application** have any **Artificial Intelligence (AI)** features or functionalities?

□ Yes

□ No

□ Not Sure (please explain):

11. If yes, please list all **AI** features and functionalities here:

Data Inventory, System Inventory and Data Maps

12. Please list all **Personal Information** data elements that will be **Processed** (recommend

creating a list and including it as evidence supporting this PIA).

13. Please list all **IT Systems** and **On-line Applications** associated with the subject of this PIA (recommend creating a list and including it as evidence supporting this PIA).

14. Please attach a data flow map that illustrates the flow of **Personal Information** through the data lifecycle, including all applicable **IT Systems**, **On-line Applications**, internal roles and third parties (recommend creating a data flow map and including it as evidence supporting this PIA).

15. Please provide any written and current external privacy notices or external privacy policies you deliver to **Data Subjects** (recommend creating a list and including it as evidence supporting this PIA).

Notice

(Utah Code § 63D-2-103, Utah Admin. Code 895-8, and Utah Code §§ 63G-2-601(2), 63D-2-103(2)-(3), and 63A-19-402)

16. Do you provide notice to **Data Subjects** before collecting **Personal Information** directly from the **Data Subject**?

□ Yes

□ No

□ N/A (please explain):

If yes, please describe how and where the notice(s) is delivered and include the substance of the notice(s) as evidence:

If not, please move on to question 17.

17. Do you provide notice to **Data Subjects** before collecting **Personal Information** indirectly (i.e. not from the **data subject**)?

□ Yes

□ No

□ N/A (please explain):

If yes, please describe how and where the notice(s) is delivered and include any URLs and the substance of the notice(s) as evidence:

If not, please move on to question 18.

Purpose Limitations

(Utah Code § 63A-19-401(2)(c)) and Utah Code Utah Code § 63A-19-402

18. Will existing **Personal Information** be used for a new purpose?

□ Yes

□ No

□ Not Sure (please explain):

19. What is your purpose for the **Processing** (select all that apply)?

□ Audits and Inspections: Verifying compliance with standards, laws, and policies.

□ Border Control and Immigration: Managing immigration, customs, and border security.

□ Census and Population Studies: Collecting demographic data to allocate resources and plan infrastructure.

□ Cultural Preservation: Maintaining archives, libraries, and museums.

□ Crisis Communication: Providing updates and information during emergencies or disasters.

□ Digital Identity and Authentication: Enabling access to government services through digital platforms.

□ Economic and Social Research: Understanding trends to design economic and social interventions.

□ Education Administration: Managing student records, attendance, and performance data.

□ Elections and Democratic Processes: Voter registration, election management, and vote processing.

□ Emergency Response: Coordinating disaster relief and public safety in emergencies.

□ Employment and HR Management: Managing government employee records, payroll, pensions, and benefits.

□ Fraud Prevention and Detection: Identifying and mitigating fraudulent activities in public programs and benefits.

□ Identity and Citizenship Management: Issuing IDs, passports, driver's licenses, and maintaining birth, marriage, and death registries.

□ Infrastructure Development: Managing transportation, utilities, and urban planning.

□ Law Enforcement and Public Safety: Criminal investigations, maintaining public safety, and enforcing laws.

□ Licensing and Permitting: Granting business, construction, and other permits or licenses.

□ National Security: Intelligence gathering, surveillance, and counterterrorism activities.

□ Policy Development and Evaluation: Analyzing data to inform policy decisions and program improvements.

□ Public Consultation and Participation: Engaging citizens in policy-making, surveys, or town hall meetings.

□ Public Health Management: Managing pandemics, monitoring disease outbreaks, and providing vaccinations.

□ Public Service Delivery: Providing essential services such as healthcare, education, social services, and housing.

□ Regulatory Oversight: Enforcing laws and regulations in areas like environmental protection, financial regulation, and consumer rights.

□ Subsidy and Benefit Distribution: Allocating financial support for eligible citizens or businesses.

□ Taxation and Revenue Collection: Collecting and managing taxes, fees, and other government revenues.

□ Transparency and Accountability: Responding to public records requests and ensuring government accountability.

□ Website and Service Analytics: Monitoring and improving government websites and e-services.

□ Worker and Public Safety: Monitoring and promoting workplace and public safety standards.

□ Other (please describe):

Data Minimization, Accuracy and Completeness

(Utah Code § 63A-19-401(2)(c)), Utah Code §§ 63G-2-603 and 63A-19-403

20. Have you collected more **Personal Information** than is needed for the purpose(s) identified above?

□ Yes

□ No

□ Not Sure (please explain):

If you have collected more information than is needed for the purpose listed above, go to question 21.

If you have not collected more information than is needed for the purpose listed above, go to question 22.

21. If you have collected more **Personal Information** than is needed, please describe the specific **Personal Information** you have collected that exceeds the purpose(s) described above. Describe here:

22. How will you maintain the accuracy and completeness of the **Personal Information** you have collected? Describe here:

Data Transfers

Utah Code §§ 63A-19-401(2)(h), 63G-2-206, and 63G-2-202(8)

23. Will the data be transferred outside your organization?

□ Yes

□ No

□ Not Sure (please explain):

If yes, go to Question 24.

If not, go to Question 28.

24. Will the data be transferred to (select all that apply):

□ Governmental entity

□ Non-governmental entity

□ Not Sure (please explain):

25. What is the purpose(s) for the transfer(s)? Please describe:

26. Will your organization receive any benefit for the transfer? Please describe:

27. Will you be monitoring and testing the other organization's processing, including disposition of the data at the end of the associated contract.

Data Storage

Utah Code §§ 63A-19-401(2)(h), 63G-2-206, and 63G-2-202(8)

28. Where will the **Personal Information** be stored (This should correspond with the data maps you have provided above)?

□ On-premises

□ Third Party Cloud Provider

□ Hybrid Solution

29. If your organization is storing **Personal Information** with a third party cloud provider do you know where your encryption/decryption keys are stored?

□ Yes

□ No

□ Not Sure (please explain):

If yes, please provide the name of the people in your organization responsible for the keys:

30. Will the data be stored in the United States?

□ Yes

□ No

□ Not Sure (please explain):

Data Security

Information Security Policy 5000-0002

31. Has your organization completed a DTS Security Review?

□ Yes

□ No

□ Not Sure (please explain):

If yes, please attach as evidence to this PIA.

If not, please go to question 32.

32. Do you have an incident response plan with a breach notification plan?

□ Yes

□ No

□ Not Sure (please explain):

If yes, please attach as evidence for this PIA.

If not, please go to Question 33.

Data Retention

Utah Code §§ 63G-2-604(1)(b) and 63A-19-404

33. How long will Personal Information be retained for the purpose described above according to the associated record series (this should align with the Retention Schedule for the associated record series)? This includes any back-up copies.

□ < 30 days

□ 30 days - 90 days

□ 90 days - 6 months

□ 6 months

□ 1 year

□ 5 years

□ 7 years

□ 10 years

□ Indefinitely

34. How long will Personal Information be retained for legal (or other) reasons according to the associated record series Retention Schedule?

□ < 30 days

□ 30 days - 90 days

□ 90 days - 6 months

□ 6 months

□ Indefinitely

Data Disposition

Utah Code §§ 63G-2-604(1)(b) and 63A-19-404

35. How will the **Personal Information** your organization is responsible for be disposed of? Please describe and highlight in the data flow maps you have provided:

Data Subject Rights

Utah Code §§ 63G-2-202(1)(a) and 63G-2-206(7), Utah Code §§ 63G-2-603 and 63A-19-403, Utah Code §§ 63G-2-601(3) and 63A-19-402(2), Utah Code § 63G-2-303.

36. Do you provide **Data Subjects** with the ability to **Access** the **Personal Information** your organization processes?

☐ Yes

☐ No

☐ Not Applicable (please explain):

37. Do you provide **Data Subjects** with the ability to **Correct** the **Personal Information** your organization processes?

☐ Yes

☐ No

☐ Not Applicable (please explain):

38. Do you provide **Data Subjects** with the ability to request an **Explanation** about the organization's processing of private or controlled records?

☐ Yes

☐ No

☐ Not Applicable (please explain):

39. Do you provide **Data Subjects** with the ability to Opt-Out of Receiving Marketing Communications from your organization?

☐ Yes

☐ No

☐ Not Applicable (please explain):

40. How do **Data Subjects** learn about how to exercise the rights available to them (i.e. receive notice)? Please describe in detail and highlight in the relevant data maps your organization has provided in this PIA:

41. How do **Data Subjects exercise** these interests (process question)? Please describe:

At Risk Employees

Utah Code § 63G-2-303

42. Do you provide At Risk Employees the right to restrict access to their Personal Information?

□ Yes

□ No

□ Not Applicable (please explain):

43. How do **Data Subjects** learn about how to exercise the rights available to them (i.e. receive notice)? Please describe in detail and highlight in the relevant data maps your organization has provided in this PIA:

44. How do **Data Subjects** exercise these interests (process question)? Please describe:

Risk Assessment

The next step is to assess the risks associated with each section above. The following table provides a custom assessment formula specific to processing of **Personal Information** by **Governmental Entities** in the State of Utah under current Utah law. Each row in the Risk Assessment table below stands-alone (i.e. this is not a cumulative assessment) for the purpose of identifying ways to lower risks associated with each section of the PIA:

Section Name	Low	Medium	High	First Ranking (low, medium or high)	Amended Ranking (low, medium or high)
Scope, Screening Questions, Data Inventory, System Inventory, Data Maps	There is no **personal information** that contains: ● children's data ● public safety or criminal convictions ● health data ● financial data ● data from incompetent Individuals, or ● other sensitive personal	There is no identifiable **personal information** that contains: ● children's data ● public safety or criminal convictions ● health data ● financial data ● data from incompetent Individuals, or	There is identifiable **personal information** that contains: ● children's data ● public safety or criminal convictions ● health data ● financial data ● data from incompetent	TBD	TBD

	information, or any large scale processing.	● other sensitive personal information, or any large scale processing.	Individuals, or ● other sensitive personal information, or any large scale processing.		
Notice	Notice is provided before collection of **Personal Information** in a Privacy Policy and Privacy Notice as required by law.	Notice is provided after collection of **Personal Information** in a Privacy Policy and Privacy Notice as required by law.	Notice is not provided before collection of **Personal Information** in a Privacy Policy and Privacy Notice as required by law.	TBD	TBD
Purpose Limitations	Purpose for collection of **Personal Information** is authorized by law as described in this PIA.	Purpose for collection of **Personal Information** is authorized by rule as described in this PIA.	Purpose for collection of **Personal Information** is not authorized by law or rule.	TBD	TBD
Data Minimization, Accuracy and Completeness	Collect only **Personal Information** required for the purpose for which it was collected.	Collect more **Personal Information** than required for the purpose for which it was collected.	Collect more **Personal Information** than needed for the purpose for which it was collected and/or is used for secondary purposes.	TBD	TBD
Data Transfers	No **transfers** of **Personal Information** outside the organization.	**Transfers** of **Personal Information** to only Governmental Entities as authorized by	**Transfers** of **Personal Information** to non-Governmental Entities, or Governmental Entities not	TBD	TBD

		law.	authorized by law.		
Data Storage	**Personal Information** stored on-premise.	**Personal Information** stored in the Cloud w/3rd Party vendor in the U.S.	**Personal Information** stored in the Cloud w/3rd Party vendor outside the U.S.	TBD	TBD
Data Security	**DTS Security Review** is complete and **Incident Response Plan** (including **Business Continuity Plan**) is in place and operationalized.	No **DTS Security Review** is complete but **Incident Response Plan** (including **Business Continuity Plan**) is in place and operationalized.	No **DTS Security Review** is complete and no **Incident Response Plan** (including **Business Continuity Plan**) is in place and operationalized.	TBD	TBD
Data Retention	**Retention Schedule(s)** approved for all **Records Series** that are operationalized and maintained.	Some **Retention Schedule(s)** approved for all **Records Series** and are operationalized and maintained.	No **Retention Schedule(s)** approved for all **Records Series** and none are operationalized or maintained.	TBD	TBD
Data Disposition	**Personal Information** disposed of in accordance with the associated retention schedule.	Some **Personal Information** disposed of in accordance with the associated retention schedule.	No **Personal Information** disposed of in accordance with the associated retention schedule.	TBD	TBD
Data Subject Rights	All legally required rights provided as required by applicable law and appropriate notice given.	All legally required rights provided as required by applicable law and no appropriate notice given.	**Some or none of the legal required rights are provided and no notice given.**	TBD	TBD

Safeguards to be Operationalized

Based on your risk assessment above, any high risk processing that is identified should be mitigated. The mitigations you identify below should lower your risk rating from high to low or medium. The identified mitigations must then be operationalized, and this PIA should be updated by listing your "amended" risk rating in the table above. A sample table for you to list all mitigations you operationalize is provided below. This table must be retained with this PIA:

PIA Section	First Risk Ranking	Identified Risk and Safeguards (describe in detail)	Evidence of Operationalization in Support of Amended Ranking
TBD	TBD	TBD	TBD
TBD	TBD	TBD	TBD
TBD	TBD	TBD	TBD
TBD	TBD	TBD	TBD

Definitions

The following definitions are specific to this PIA Template:

- **Aggregated Data** is Personal Information that has been combined to show patterns, statistics or trends associated with Data Subjects. The Aggregated Data cannot identify the Individual Data Subjects who provide the source data.
- **Access** is a Data Subject right that requires your organization to provide each Individual requestor with access to the Personal Information your organization Processes.
- **Anonymized Data** is data that is no longer possible to identify Individual Data Subjects. Whether Personal Information is truly anonymized should be confirmed by a subject matter expert.
- **Correction** is a Data Subject right that requires your organization to facilitate each Individual requestor's request to correct the Personal Information your organization Processes.
- **Data Subject** is the living Individual that is the subject of the Personal Information you are Processing. Processing is anything the organization may do with Personal information throughout the lifecycle of the data.
- **Deidentified Personal information** is any personal information that has been altered for the purpose of making it harder to identify the Data Subject, e.g. removal of name, address and phone number, hashing, encryption, salting, block chain, aggregation, etc.

- **Explanation** is a Data Subject right that requires your organization to provide an explanation to each Individual requestor's request for information about the private or controlled record(s) your organization Processes.
- A **Governmental entity** is an executive department agency of the state, offices of the governor, lieutenant governor, state auditor, attorney general and state treasurer as well as the entities listed in Utah Code 63A-19-101(7) and 63G-2-103(11))
- **High Risk Processing** is processing of personal information that may result in a significant compromise to an individual's privacy rights, based on factors that include the sensitivity, amount, risk of unauthorized access or use, and whether consent has been obtained for the processing (Utah Code 63A-19-101(8)).
- An **Individual** is a natural living person (Utah Code 63A-19-101(9) and 63G-2-102(12).
- **IT System** is any digital system that processes the Personal Information identified in this PIA.
- **On-line Application** is any digital application that Processing the Personal Information identified in this PIA.
- **Personal Information** is any information (or data) relating to an identified or identifiable Individual and includes personally identifying information (Executive Order 2023-06).
- **Sensitive Personal Information** is any Personal Information that will likely introduce a high risk to the rights and freedoms of a Data Subject. Sensitive Personal Information is a sub-set of Personal Information.
- **Process or Processing** is any operation or set of operations performed on personal information as defined in Utah Code 63A-19-101(14).
- **Product** - is an offering delivered by your organization to the clients named in your enabling statute or other regulatory mandate that is a tangible good.
- A **Sale (or Sell)** means an exchange of personal data for monetary consideration by a governmental entity to a third party. A Sale does not occur when a governmental entity charges a fee for access to a record or a fee assessed in accordance with an approved fee schedule (Utah Code 63A-19-101(18)).
- **Service** is an offering delivered by your organization to the clients named in your enabling statute or other regulatory mandate that is NOT a tangible good.
- **Sharing** personal information occurs when you Transfer personal information to another entity (including another government entity) without monetary compensation.
- **State Agency** is an entity under the direct supervision and control of the governor or the lieutenant governor from the list of entities listed in Utah Code 63A-19-101(19). A State Agency does not include the legislative or judicial branch, an independent entity, or an executive agency within the Office of the Attorney General, the state auditor, the state treasurer, or the State Board of Education.
- A **Transfer** occurs when you Share or Sell personal information to another entity, which includes other government entities.