# STATE OF UTAH

# Office of Data Privacy

# Privacy Impact Assessment

Version 1.1

Utah Office of Data Privacy
Privacy Impact Assessment
(IT Systems)

## Purpose

This Privacy Impact Assessment(PIA) is designed as a guide for governmental entities to assess compliance with the applicable privacy practice obligations detailed in the Privacy Program Framework from Utah's Office of Data Privacy. The PIA helps to identify privacy risks to the individuals for which entrusted governmental entities with personal data for processing. Once the impact on and risks to individuals' privacy are identified, the governmental entity is directed to identify specific actions (safeguards) the organization will take to lower these impacts and risks to individuals' privacy that have been identified. The overall intent of the PIA is to ensure governmental entities are compliant with the data privacy requirements in the GDPA, GRAMA, and DARS.

## Application and Authority

This PIA, established by the CPO and approved by the CIO, is required to be completed by all state agencies for any information technology that processes personal data. *See* DTS Information Security Policy 5000-0002.2.4.3.1. This PIA must be completed prior to:

- developing or procuring new information technology that process personal data; and
- initiating a new collection or processing activity of personal data in existing information technology.

The CAO of each state agency must ensure that a PIA is completed and maintained for a minimum of four years.

**CHANGE LOG**

| Version | Date | Author | Description of Changes |
|---|---|---|---|
| 1.0 | 06.09.2025 | George McEwan | Initial release |

| | | | |
|---|---|---|---|
| 1.1 | 6-23-2025 | George McEwan | Q16 modified to reflect GDPA |

Definitions

1) "Artificial Intelligence" or "AI" means any machine-based system that can perform tasks normally requiring human intelligence, such as data analysis, pattern recognition, prediction, or decision-making.
2) "Accurate" means the information is factually true and current.
3) "Complete" in the context of this PIA, means personal data is not missing critical information that could lead to misinterpretation or incorrect decisions.
4) "At-risk employee" means a government employee who, because of the unique nature of the employee's regular work assignments or because of one or more recent credible threats directed to or against the employee, would be at immediate and substantial risk of physical harm if the employee's personal information is disclosed. Utah Code § 63G-2-303
5) "Chief administrative officer" or "CAO" means the individual designated by a governmental entity to perform the duties of records management as detailed in Utah Code § 63A-12-103 .
6) "Chief Information Officer" or "CIO" means the chief information officer appointed under Section 63A-16-201. This role is housed in the Division of Technology Services.
7) "Chief Privacy Officer" or "CPO" means the individual appointed under Section 63A-19-302. This role provides oversight and guidance to all governmental entities in the state on matters of privacy. The CPO role is housed in the Office of Data Privacy.
8) "Compensating Control" means a documented procedure or practice that is used to mitigate an identified risk.
9) "DARS" means the Division of Archives and Records Service and Management of Government Records found at Utah Code § 63A-11-100.5 et seq.
10) "De-identified" means information from which personal data has been removed or obscured so that the information is not readily identifiable to a specific individual, and which may not be re-identified.
11) "Division of Technology Services" or "DTS" means the Division of

Technology Services created in Utah Code § 63A-16-103.

12) "Document artifacts" means supporting evidence which may take the form of data flow diagrams, network architecture diagrams, APIs, data schemas, and user interface specifications.
13) "Executive branch agency" means an agency or administrative subunit of state government Utah Code § 63A-16-102. The legislative branch and the judicial branch are not considered executive branch agencies.
14) "GDPA" means the Government Data Privacy Act found at Utah Code § 63A-19-101 et seq.
15) "Governmental entity" in the context of this PIA, refers to any entity that is funded by or established by the government to carry out the public's business. Utah Code § 63G-2-103.
16) "GRAMA" means the Government Records Access and Management Act found at Utah Code § 63G-2-103 et seq.
17) "High risk processing activity" means a governmental entity's processing of personal data that may have a significant impact on an individual's privacy interests. See Utah Code § 63A-19-101(17).
18) "Incapacitated individuals" means an adult's ability to do the following is functionally impaired to the extent that the individual lacks the ability, even with appropriate technological assistance, to meet the essential requirements for financial protection or physical health, safety, or self-care. Reference Utah Code § 75-1-201(25) for additional information.
19) "Information technology" means the same as defined in Utah Code § 63A-16-102.
20) "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual. Utah Code § 63A-19-101(24).
21) "Personal information" means the employee's or the employee's family member's home address, home telephone number, personal mobile telephone number, personal pager number, personal email address, social security number, insurance coverage, marital status, or payroll deductions. See Utah Code § 63G-2-303.
22) "Policy" means the DTS Information Security Policy 5000-0002.
23) "Privacy Impact Assessment" or "PIA" means an analysis of how personal data is processed by information technology to ensure that processing conforms with applicable privacy requirements and assists in identifying

privacy risks that may need to be mitigated and includes both an analysis and a formal document that details the process and outcome of the analysis.

24) "Process," "processing," or "processing activity" 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. Utah Code § 63A-19-101(27).

25) "Records officer" or "RO" means the individual appointed by the chief administrative officer of each governmental entity, or the political subdivision to work with state archives in the care, maintenance, scheduling, designation, classification, disposal, and preservation of records. Utah Code § 63G-2-103.

26) "Sell" means an exchange of personal data for monetary consideration by a governmental entity to a third party. This does not include fees for access to a record, in accordance with an approved fee schedule. Utah Code §63A-19-101(33).

27) "Sensitive personal data" means the same as defined in Utah Code § 13-61-101(32), which is data that reveal characteristics of an individual such as race, religion, sexual orientation, citizenship or immigration status, or information related to health history both physical and mental conditions.

28) "State Privacy Auditor" means the individual appointed by the state auditor who performs the auditing functions as related to the GDPA; specific duties of the role are defined in Utah Code § 67-3-13.

29) "User data" means any information about a user that is automatically collected by a government website when a user accesses the government website. This can include materials requested from the website, specifics about the user's device (i.e. browser type, IP address, device fingerprints, etc) for a complete definition reference Utah Code § 63A-19-101(38).

30) "Utah Office of Data Privacy" or "ODP" means the Utah Office of Data Privacy created in Utah Code § 63A-19-301.

## Guidance

Your completed PIAs may be managed as part of Retention Schedule **GRS-1713** if your entity does not have a specific record series created to manage them. This Retention Schedule aligns with the requirement to keep the PIAs for four years as outlined above and/or as long as the processing occurs.

The CAO named below is ultimately responsible for the factual accuracy of the information contained within this PIA and attests to its completion by signing and dating this document. If your entity has CAO and RO duties assigned to one person, the attestation is still made by the role of CAO.

Any document artifacts requested in the PIA which are classified by the governmental entity as protected, private, or controlled (Utah Code § 63G-2-3) as defined in GRAMA must be included by reference and be available for inspection upon request by the ODP for high risk monitoring purposes Utah Code § 63A-19-301(3)d

As mentioned in the introduction, questions in the PIA are designed to help governmental entities lower privacy risks to personal data and ensure compliance with the GDPA. If you are unsure how to respond to a question in the PIA, the ODP is available to answer questions and provide training on completing the PIA. You can contact us directly at: officeofdataprivacy@utah.gov,or https://privacy.utah.gov/.

## General Information

Name of governmental entity: _____

Name of the information technology _____

Include the records series which applies to the personal data processed by the information technology in scope for this PIA: _____

Include the retention schedule that has been applied to the record series which has been approved by the State Records Management Committee which

applies to the personal data processed by the information technology in scope for this PIA: _____

List the statutes or legal authority that authorize your organization to process the personal data: _____

Name of the CAO who will approve this PIA: _____

Name(s) of the person(s) and title(s) who completed this PIA: _____

## Governmental Entity Demographics

Provide a brief description of the product or services your governmental entity provides: _____

Number of people served annually by your governmental entity: _____

Anticipated or known number of individuals that are served annually by the information technology in scope for this PIA: _____

Number of employees assigned to the support the information technology in scope for this PIA: _____

## Screening Questions

1. Is this a new information technology or are you modifying an existing information technology?

☐ New information technology

☐ Modifying existing information technology

If this is a new information technology, briefly describe its functionality as related to the service offering provided by the governmental entity.

If this is a modification to an information technology, include by reference any prior PIAs completed for the information technology and describe what is changing or being added to the existing information technology in this PIA.

2. Will the information technology be processing personal data, regardless of whether it is de-identified or not?

- ☐ Yes
- ☐ No

If yes, proceed to question 3.

If not, there is no need to conduct a PIA. Please assign a record series to this document (Retention Schedule GRS-16597) and store this assessment in the appropriate file. STOP here.

3. What is the relationship between your governmental entity and the individual (select all that apply)?

- ☐ Resident
- ☐ Website visitor
- ☐ Employee
- ☐ Contingent Worker (3rd Party)
- ☐ Independent Contractor (3rd Party)
- ☐ Strategic Partner (3rd Party)
- ☐ Other (please describe):

4. Please select the approximate number of individuals' personal data which will be processed by the IT system.

- ☐ < 500 Individuals
- ☐ 500-<10,000 Individuals
- ☐ 10,001 - <100,000 Individuals
- ☐ 100,001 - <1 million Individuals (large scale processing)
- ☐ 1 million Individuals or more (large scale processing)

5. Please select the approximate age range of the individuals' personal data which will be processed by the IT system.

(select all that apply).

- ☐ < 13 years of age
- ☐ 13 - < 18 years of age
- ☐ 18 - < 65 years of age
- ☐ 65 years of age or older

6. How is personal data collected (select all that apply)?
   - ☐ Directly from the individual
   - ☐ Indirectly from a public source
   - ☐ Indirectly from another government entity
   - ☐ Indirectly from a non-government entity (3rd party)
   - ☐ Other (please describe):
7. Do you collect sensitive personal data or personal data from incapacitated individuals?
   - ☐ Yes
   - ☐ No
   - ☐ Not Sure (please explain):
8. Does your IT System have any AI features or functionalities?
   - ☐ Yes
   - ☐ No
   - ☐ Not Sure (please explain):

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

Data Inventory, System Inventory and Data Maps

9. Please list all personal data and user data that is in scope for this PIA.

10. Please list all information technology which connects to the information technology which is the subject of this PIA, including IT that is used by a service provider whose system is within the scope of this PIA (Typical artifacts may include: System Architecture Diagrams, Network Topology Diagrams, Interface Control Documents (ICDs or APIs), and Configuration Management Database inventory lists)

11. Include a data flow map that illustrates the flow of personal data through the data lifecycle, including all applicable information technology and third parties

12. Please provide a list of all information technology administrative roles and business roles which will have access to the personal data.

Privacy Notice

13. Do you provide a privacy notice to individuals that is fully compliant with Utah Code § 63A-19-402 and clearly states in plain language the following:

    a. all intended purposes and uses of the personal data;
    b. the consequences for refusing to provide the personal data;
    c. the classes of persons and governmental entities;
        i. with whom the governmental entity shares personal data; or
        ii. to whom the governmental entity sells personal data; and
    d. the record series in which the personal data is included.

☐ Yes

☐ No

☐ N/A (please explain):

14. If you meet the criteria in Utah Code § 63A-19-402(5), the privacy notice may be posted on the public notice website otherwise it must be posted on the governmental entity. Where is your privacy notice posted:

☐ Posted on governmental entity's website; or

☐ Posted on the public notice website?

If posted on the government entity's website, provide a link to the privacy notice as evidence:

If posted on the public notice website, the CAO is attesting to the fact the government entity does not have a government website. Provide a link to the posting on the public notice website as evidence.

15. Do you provide individuals with the ability to request an explanation about the information contained in the privacy notice as required by Utah Code § 63G-2-601(3)?

☐ Yes

☐ No

☐ Not Applicable (please explain):

16. Do you have a process for data subjects to request a privacy notice for data previously provided by the data subject? Utah Code § 63A-19-402(6)?

☐ Yes

☐ No

☐ Not Applicable (please explain):

## Website Privacy Notice

17. Do you provide a website privacy notice to users which is fully compliant with Utah Code § 63A-19-402.5(1) which clearly states in plain language the following:

a. the identity of the governmental entity responsible for the government website;
b. how to contact the governmental entity that is responsible for the government website;
c. the method by which a user may:
    i. seek access to the user's personal data or user data;
    ii. request to correct or amend the user's personal data or user data;

iii. file a complaint with the data privacy ombudsperson; and

d. how an at-risk employee may request that the at-risk employee's personal information be classified as a private record under Section Utah Code § 63G-2-302?

☐ Yes

☐ No

If yes, please describe how and where the notice is provided and include a copy of the notice as evidence:

18. If the website collects user data, is the website privacy notice fully compliant with Utah Code § 63A-19-402.5(2) which in addition to items in question 17, it clearly states in plain language the following:?

a. any website tracking technology that is used to collect user data on the government website;
b. what user data is collected by the government website;
c. all intended purposes and uses of the user data;
d. the classes of persons and governmental entities:
   i. with whom the governmental entity shares user data; or
   ii. to whom the governmental entity sells user data; and
e. the record series in which the user data is included.

☐ Yes

☐ No

If yes, please describe how and where the notice is provided and include a copy of the notice as evidence:

19. Is the website privacy notice prominently posted in compliance with Utah Code § 63A-19-402.5 by being posted as:

1. The full text of the notice on the homepage of the governmental website; or
2. link to a separate webpage containing the notice;

☐ Posted either on homepage or separate link

☐ Not posted

If posted, provide a link to the notice

Purpose Limitations

20. Will personal data you previously obtained be used for a new purpose?

☐ Yes

☐ No

☐ Not Sure (please explain):

If yes, proceed to question 21

If not, proceed to question 22

21. Has a privacy notice for the new use of the existing data been provided to the individual who supplied the personal data ?

☐ Yes

☐ No

☐ Not Sure (please explain):

If yes, proceed to question 22

If not, the use of the personal data previously furnished by the individual is not authorized under the GDPA. Your governmental entities should take steps to ensure the new use of the existing personal data by the information technology meets the provisions detailed in Utah Code § 63A-19-402. Proceed to question 22.

22. Is the information technology processing new personal data in compliance with the stated purposes in the privacy notice (Utah Code § 63A-19-402) which has been supplied to the individual?

☐ Yes

☐ No

☐ Not Sure (please explain):

If yes, briefly describe the new processing activity and then proceed to question 23

If not, your governmental entity may not be in compliance with GDPA and should not use the new personal data until a privacy notice has been provided to the individual which states in plain language the use of the new personal data. Proceed to question 23.

23. What is the purpose for processing the personal data (select all that apply)?

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

☐ 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, 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.
- ☐ 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

24. Do you collect more personal data than is reasonably necessary to efficiently achieve the specified purposes identified above?

☐ Yes

☐ No

☐ Not Sure (please explain):

If yes, go to question 25.

If not, go to question 26.

25. If you collect more personal data than is reasonably necessary, please describe the specific personal data you collect that is not reasonably necessary. If your entity has a minimization plan to dispose of the personal data which is not necessary, please describe:

26. Describe your methodology for ensuring the accuracy and completeness of the personal data collected.

## Data Sharing

27. Is your governmental entity sharing personal data within the scope of this PIA?

☐ Yes

☐ No

28. Pursuant to Utah Code § 63A-19-401 provide your statutory basis to share

the personal data:

29. Do you maintain a list of the names and contact information for the entities with whom you share information?

If yes, please provide the storage location where the information is kept.

30. Who is the personal data shared with (select all that apply):

☐ Governmental entity

☐ Non-governmental entity

31. Detail out the names and contact information for the entities with whom your entity is sharing the personal data.

32. Describe the intended use of the personal data by the other entity.

33. List all data elements which will be shared.

34. Provide notation as to the length of time your entity is obligated to share the personal data.

35. Describe the final disposition of the data shared with the other entity when the sharing agreement terminates.

Data Selling

36. Is your governmental entity selling personal data within the scope of this PIA?

☐ Yes

☐ No

37. Pursuant to Utah Code § 63A-19-401 provide your statutory basis to sell the personal data.

38. Who is the personal data being sold to? Please select all that apply:

☐ Governmental entity

☐ Non-governmental entity

39. Do you maintain a list of the names and contact information for the entities with whom you sell information?

If yes, please provide the storage location where the information is kept.

40. List all data elements which will be sold.

41. Describe the intended use of the personal data by the external entity.

42. Provide notation as to the length of time your entity will be selling personal data.

43 Describe the final disposition of the data sold to the other entity when the agreement terminates.

## Personal Data Purchasing

44. Is your governmental entity purchasing personal data within the scope of this PIA?

☐ Yes

☐ No

45. What is the source of purchased personal data? Please select all that apply:

☐ Governmental entity

☐ Non-governmental entity

46. Explain the justification for purchasing personal data.

47. List all data elements being purchased.

48. Detail how the personal data will be used in your governmental entity's process.

49. Provide an attestation that your entity is purchasing only enough personal data to reasonably achieve the specified purpose

50. If the external entity is providing more data that is needed, detail how your entity will dispose of the unneeded data.

51. If there are specific dispositions of purchased personal data when the agreement between the parties terminates, describe the actions your entity

will take to be compliant with the terms of the agreement.

## Contractor Agreement/Contracts

52. Does your governmental entity have any agreements with non-governmental entities to process personal data within the scope of this PIA?

- ☐ Yes
- ☐ No
- ☐ Not Sure (please explain):

If yes, please provide the storage location where the information is. List what personal data elements are processed with the external entity. Proceed to question 51.

If not, proceed to question 52.

53. Do you include in your contract standard terms and conditions the requirements for contractors contained in Utah Code § 63A-19-401.4 ?

- ☐ Yes
- ☐ No
- ☐ Not Sure (please explain):

## Data Storage

54. Where is the personal data stored? (This should correspond with the data maps you have provided above)

- ☐ On-premises
- ☐ Third Party Cloud Provider
- ☐ Hybrid Solution

55. For any personal data not stored on-premises, do you have legal agreement with third-party providers that ensure no State-owned data is stored or processed outside the continental United States?

☐ Yes

☐ No

☐ Not Sure (please explain):

56. If your organization is storing personal data with a third party cloud provider does your entity maintain exclusive control over all encryption/decryption keys?

☐ Yes

☐ No

☐ Not Sure (please explain):

If yes, please provide a list of the names and positions of all individuals who have positive control of the keys.

If not, please list the compensating control to ensure the keys are not being misused by a third party (i.e. immutable logging for key access, or other preferable controls from the NIST 800-53 Security and Privacy Controls for Information Systems and Organizations)

## Data Security

57. Has your governmental entity completed a DTS Security Review for the information technology described in this PIA as required by DTS Information Security Policy 5000-0002?

☐ Yes

☐ No

☐ Not Sure (please explain):

If yes, please attach as evidence to this PIA.

58. 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.

Chief Administrative Officer (CAO) Attestation

I hereby attest that the information contained in this Privacy Impact Assessment (PIA) is complete and factually accurate to the best of my knowledge.

Name: _____

Title: _____

Agency/Department: _____

Signature: _____

Date: _____