VERSION 2.1

PRIVACY PROGRAM FRAMEWORK

Utah Office *of* Data Privacy

4315 S 2700 W, Taylorsville, UT 84129
officeofdataprivacy@utah.gov | privacy.utah.gov

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Utah Office of Data Privacy (Office), created in the Government Data Privacy Act (GDPA), under the direction of the State's Chief Privacy Officer (CPO) has been established within the Department of Government Operations.[1] The Office is directed to—among other things—assist governmental entities in meeting their privacy obligations.

Under the GDPA a governmental entity is required to initiate a data privacy program before December 31, 2025.[2] This Privacy Program Framework (Framework) is provided to entities by the Office, in part, as a resource to assist them in meeting the December 31, 2025, deadline.[3] There will be future iterations of the Framework as the content is refined and revised with stakeholder feedback, and as new and amended laws dictate.[4] The Office creates and maintains tools, training, and other resources, on its website—privacy.utah.gov—that align with this Framework. The website also contains information about efforts the Office is undertaking to assist governmental entities in meeting their privacy obligations and maturing their privacy practices. Please contact the Office with any feedback or questions with respect to this Framework.

WHAT IS A PRIVACY PROGRAM?

A data privacy program is generally considered to be the structured collection of an entity's privacy practices, policies, and procedures that govern its processing and protection of personal data[5] to ensure compliance with applicable laws.[6] A data privacy program will likely meet the December 31, 2025, deadline even if it is in its early stages. Additionally, governmental entities can satisfy the requirement to initiate a privacy program by fulfilling the reporting requirements under Section 63A-19-401.3, see *infra* Privacy Practice 1.5. Entities may choose to adopt this Framework as a foundational part of their program. The Framework consists of privacy practices based on generally applicable legal requirements, a maturity model for measuring the maturity of practices to inform an entity's strategies to improve maturity, and a recommended approach of, "Ready, Set, Go!", that entities may adopt as a reasonable approach to initiate and prioritize privacy practice implementation.

This approach aligns with the December 31, 2025, requirement by providing a roadmap for entities to initiate, at a minimum, an incipient data privacy program. Over time, entities can increase the maturity of their data privacy program, while considering their available resources, the current maturity of their privacy practices, and their strategies for advancing operational complexity and effectiveness.

PRIVACY PROGRAM FRAMEWORK

LAWS

This Framework is aligned with Utah's generally applicable data privacy laws and administrative rules for governmental entities. All governmental entities are required to have a data privacy program with adequate privacy practices that also account for entity-specific, state, and federal laws or regulations.

PRIVACY PRACTICES

This Framework includes 23 privacy practices the Office has identified through its analysis and interpretation of generally applicable Utah law. Part 1 provides a summary analysis, description, and legal basis of each practice. Tools and resources associated with a privacy practice can be found on privacy.utah.gov. The practices are grouped and numbered according to the NIST Privacy Framework's categories: Govern, Identify, Control, Communicate, and Protect.

PRIVACY MATURITY MODEL AND STRATEGIES

This Framework includes a maturity model that entities can use to measure the maturity of their data privacy practices and programs. Based on these assessments, entities should then develop and document strategies to increase the maturity of their practices and programs over time. Details about the privacy maturity model are in Part 2 of this Framework. Individual practice-specific maturity models are being developed and will be added to this Framework in future versions.

READY, SET, GO APPENDIX

Guidance for initiating the development of your privacy program.

PRIVACY MATURITY MODEL

5 — OPTIMIZED
The practice is fully embedded in the entity with recognition and understanding across the work-force through active training and awareness campaigns, and inclusion in operations and strategy.

4 — MANAGED
The practice is actively managed with metrics that are reviewed to assess efficacy and facilitate improvement.

3 — CONSISTENTLY IMPLEMENTED
The practice is documented to cover all relevant aspects, application is formal and consistent.

2 — DEFINED
The practice is implemented and documented, but documentation may not cover all relevant aspects, and application may be informal and inconsistent.

1 — AD HOC
The practice may occur but is undocumented (no policies or procedures), application is reactive and not standardized.

0 — NON-EXISTENT
The practice is not implemented or acknowledged.

INTRODUCTION TO THE FRAMEWORK

This Framework is aligned with Utah law and administrative rules that are generally applicable across governmental entities with respect to data privacy. It also highlights differences between state agencies and political subdivisions where they exist. By December 31, 2025, all governmental entities are expected to have initiated a data privacy program with privacy practices that also account for entity-specific laws, regulations, or ordinances, including governing federal laws and regulations.

Requirements for the privacy practices of governmental entities are spread across various state, federal, and local laws. The Government Data Privacy Act[7] (GDPA) represents an initial, incremental step toward standardizing and consolidating privacy requirements for governmental entities.

As this long-term process unfolds, entities generally remain subject to the data privacy practice requirements in Title 63G, Chapter 2, Government Records Access and Management Act (GRAMA), and Title 63A, Chapter 12, Division of Archives and Records Service and Management of Government Records (DARSMGR).[8] Although often seen as record access and management laws, they also contain privacy practices that overlap with data governance and records management practices, e.g., inventorying, classification, and disposition. This overlap allows entities to align their data privacy programs with the records management life cycle, which can improve overall data governance.

To assist with compliance, entities should familiarize themselves with their current privacy obligations and available resources. This Framework provides a high-level overview of those obligations and the resources available from the Office, as follows:

PART 1: PRIVACY PRACTICES

Current generally applicable governmental entity privacy obligations are outlined with associated guidance.

PART 2: PRIVACY MATURITY MODEL & STRATEGIES

A standard model for entities to use for internal self-assessments and measurement of privacy practice maturity to inform policy, strategy, and risk management decisions.

PART 1: PRIVACY PRACTICES

For the purposes of this Framework, privacy practices are defined as a governmental entity's organizational, technical, administrative, and physical safeguards. These include the policies and procedures an entity uses to manage personal data throughout its entire lifecycle: acquisition, use, storage, sharing, retention, and disposal. These practices also encompass the act of providing individuals with notice of their privacy interests and rights.[9] An entity must ensure its privacy practices adequately protect individual privacy, align with the State Data Privacy Policy[10], and comply with all applicable privacy laws. The practices outlined in this Framework are foundational to a robust privacy program. Entities are required to account for these practices unless a more specific, restrictive, or preempting law applies.[11]

PRIVACY PRACTICES

CATEGORY	IDENTIFIER	PRIVACY PRACTICE NAME
GOVERN	1.1	Chief Administrative Officer (CAO) Designation
	1.2	Records Officer Appointment
	1.3	Records Officer Training and Certification
	1.4	Statewide Privacy Training
	1.5	Privacy Program Report
IDENTIFY	2.1	Record Series Creation and Maintenance
	2.2	Record and Record Series Designation and Classification
	2.3	Statement Filed with State Archivist
	2.4	Retention Schedule Proposal and Approval
	2.5	Record Series Privacy Annotation
	2.6	Inventorying
	2.7	Privacy Impact Assessments (PIA)
	2.8	Record and Personal Data Sharing, Selling, and Purchasing
CONTROL	3.1	Data Subject Requests for Access
	3.2	Data Subject Requests for Amendment or Correction
	3.3	Data Subject Requests for an Explanation
	3.4	Data Subject Requests by At-Risk Employees for Restricting Access
COMMUNICATE	4.1	Privacy Notice (Notice to Provider of Information)
	4.2	Website Privacy Notice and Website Privacy Policy
PROTECT	5.1	Minimum Data Necessary
	5.2	Retention and Disposition of Records Containing Personal Data
	5.3	Incident Response and Notification to the Cyber Center and Attorney General
	5.4	Breach Notification to Affected Individuals

GOVERN

1.1 **Chief Administrative Officer (CAO) Designation**

Governmental entities are required to designate one or more CAOs.[12] The name of the designated CAO must be reported to the Division of Archives and Records Service (Archives).[13] The CAO for each governmental entity is responsible for ensuring their entity complies with the requirements of DARSMGR, GRAMA, and Part 4 of the GDPA.[14] CAO responsibilities include establishing and maintaining an active, continuing program for the economical and efficient management of the entity's records as provided by DARSMGR and GRAMA.[15] Additionally, the CAO is mandated to create and maintain documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the entity.[16] Tvhis documentation must be designed to furnish information that protects the legal and financial rights of persons directly affected by the entity's activities.[17] Thus, an entity's designated CAO is primarily responsible for creating and maintaining the policies and procedures associated with the privacy practices identified in this Framework.

Authority: Utah Code § 63A-12-103

1.2 **Records Officer Appointment**

Entity CAOs are required to appoint one or more records officers[18] responsible for ensuring the "care, maintenance, scheduling, disposal, classification, designation, access, and preservation of records."[19] A records officer is responsible for following policies and procedures created by the CAO, including those associated with the privacy practices identified in this Framework. The name(s) of a governmental entity's records officer(s) must be reported to Archives.[20]

Authority: Utah Code § 63A-12-103

1.3 **Records Officer Training and Certification**

Each records officer of an entity must annually complete online training on GRAMA provisions and obtain certification from Archives, in accordance with Section 63A-12-110.[21] An understanding of GRAMA is critical due to the overlapping relationship between records management, data governance, and privacy, which forms the foundation for an entity's privacy program. The importance of GRAMA training for privacy programs has increased with a legislative mandate for the CPO to coordinate with the State Archivist to incorporate data privacy practices into records management and the GRAMA trainings described in Section 63A-12-110.[22]

Authority: Utah Code § 63A-12-110 and 63G-2-108

1.4 **Statewide Privacy Training**

Privacy awareness training ensures employees possess the knowledge and skills to appropriately handle personal data, recognize and respond to privacy concerns, and prevent privacy incidents, thereby reducing the risk of data breaches and associated ramifications. Ultimately, privacy training and awareness programs build a privacy conscious workforce. Employees of governmental entities who have access to personal data as part of their work duties, or who supervise an employee with such access, are required to complete a data privacy training program within 30 days after beginning employment and at least once each calendar year.[23] Governmental entities are responsible for ensuring this required training is completed and for reporting compliance as described in Section 63A-19-401.3.[24]

The Office has been directed to create a data privacy training program for employees of governmental entities.[25] This training is intended to "provide instruction regarding data privacy best practices, obligations, and responsibilities; and the relationship between privacy, records management, and security."[26] Privacy awareness trainings are available on privacy.utah.gov or by contacting the Office.

Authority: Utah Code §§ 63A-19-301, 401.2, and 401.3

1.5 **Privacy Program Report**

The CAO of each governmental entity must, by December 31st annually, submit an annual privacy program report (report), in accordance with the specific requirements detailed in Utah Code § 63A-19-401.3. This report should detail whether a privacy program has been initiated and describe any implemented privacy practices, strategies for improvement, and high-risk data processing activities.[27] It needs to list the types of personal data shared, sold, or purchased, along with the legal justification for such activities, and identify the categories of individuals or entities involved.[28]

The report must also state the percentage of employees who have completed data privacy training and outline any non-compliant processing activities found and the plan to address them.[29]

This report is considered a protected record under Utah Code § 63G-2-305 and may be requested by the Office.[30]

Fulfilling the reporting requirement can satisfy the requirement for a governmental entity to initiate a privacy program by December 31, 2025.[31]

The Office has created a privacy program report draft template that a governmental entity may use as a starting point for its particular report. This can be found on the website of the Office at privacy.utah.gov.

Authority: Utah Code § 63A-12-103

IDENTIFY

2.1 **Record Series Creation and Maintenance**

Governmental entities manage and maintain records according to GRAMA's requirements.[32] GRAMA defines "record" as all electronic data, or other documentary material regardless of physical form or characteristics (including: book, letter, document, paper, map, plan, photograph, film, card, tape, recording) that is prepared, owned, received, or retained by a governmental entity (and where all of the information in the original is reproducible by photocopy or other mechanical or electronic means).[33] It's important to note that GRAMA contains a substantial list of items excluded from the definition of "record."[34]

Governmental entities then group records that can be treated as a unit for purposes of designation, description, management, or disposition into a "record series."[35] Records must be maintained according to their record series attributes, e.g., retention, classification, and purpose and use limitations.[36] GRAMA allows political subdivisions to address certain requirements through the adoption of an ordinance or policy, as detailed in Utah Code § 63G-2-701.

Authority: Utah Code §§ 63A-121-03, 63G-2-103(25) and 26, and 701

2.2 **Record and Record Series Designation and Classification**

Record and record series designation and classification are governed by both GRAMA and DARSMGR. These acts require governmental entities to evaluate and designate each record series they keep, use, or create, and to report this designation to Archives.[37] GRAMA provides distinct definitions for both *designation* and *classification*.

Designation is defined in GRAMA as: "indicating, based on a governmental entity's familiarity with a record series or based on a governmental entity's review of a reasonable sample of a record series, the primary classification that a majority of records in a record series would be given if classified and the classification that other records typically present in the record series would be given if classified."[38]

Classification is defined in GRAMA as: "determining whether a record series, record, or information within a record is public, private, controlled, protected, or exempt from disclosure under Subsection 63G-2-201(3)(b)."[39]

Although an entity "is not required to classify a particular record, record series, or information until access to the record is requested," GRAMA still requires an initial designation of a record series irrespective of whether a request has been made.[40]

Political subdivisions may adopt a jurisdiction-wide ordinance or policy for information practices, including record designation and classification.[41] If adopted, each ordinance or policy must provide standards for classification and designation of the records of the entity in accordance with GRAMA Part 3.[42] If a political subdivision does not adopt and maintain such an ordinance or policy, that entity is subject to GRAMA.[43] Political subdivisions must report to Archives all designations and classifications applied to record series they maintain.[44]

Authority: Utah Code § 63G-2-103, 307, and 701

2.3 **Statement Filed with State Archivist**

Under GRAMA, governmental entities must file a statement with the state archivist. This statement must explain the purpose for which each private or controlled record series is collected, maintained, or used.[45] It must also identify the legal authority for collecting this information.[46] This statement is a public record.[47] Governmental entities are prohibited from using private or controlled records for any purpose other than those listed in the statement or as permitted under Section 63G-2-206.[48] All uses are also subject to individual notice requirements under Subsection 63G-2-601(2) and Section 63A-19-402.

This statement and the notice requirements are redundant with provisions of the GDPA. The Office is working with the Legislature to consolidate them appropriately within the GDPA.

Authority: Utah Code § 63G-2-601

2.4 **Retention Schedule Proposal and Approval**

Governmental entities must schedule—as defined in GRAMA—the length of time each *record* and *record series* should be retained by the entity for administrative, legal, fiscal, or historical purposes and when each record series should be transferred to Archives or destroyed (commonly referred to as a retention schedule).[49] An entity must maintain and destroy records in accordance with an approved retention schedule.[50] Entities should also have retention schedules for objects not defined as a record under Section 63G-2-103, but that have historical or evidentiary value.[51]

The CAO of each governmental entity is responsible for submitting a proposed schedule for the retention and disposition of each type of material that is defined as a record under GRAMA to the State Archivist. This schedule requires final approval by the Records Management Committee (RMC), created in Section 63A-12-112.[52] Once a retention schedule is reviewed and approved by the RMC, the entity must maintain and destroy records in accordance with the approved schedule.[53] If an entity has not received an approved retention schedule for a record type, the general retention schedule maintained by the State Archivist governs its retention and destruction.[54] (Archives is mandated to "establish standards for the preparation of schedules providing for the retention of records of continuing value and for the prompt and orderly disposal of state records no longer possessing sufficient administrative, historical, legal, or fiscal value to warrant further retention.")[55]

The RMC is responsible for reviewing and determining whether to approve each schedule for record retention and disposal, and must do so within three months after submission.[56] Procedures for entities to submit and obtain RMC approval for record series retention schedules, as well as rules detailing RMC processes and schedule review and approval, are established in Utah Administrative Code R36-1-1 *et seq.* Additional information on the RMC, including current Committee Members, is available on the Division of Archives and Records Service website.[57]

Political subdivisions may adopt a jurisdiction-wide ordinance or policy for information practices, including record retention.[58] If adopted, each ordinance or policy must provide standards for record management and retention comparable to Section 63A-12-103.[59] If a political subdivision does not adopt and maintain such an ordinance or policy, that entity is subject to GRAMA.[60] Political subdivisions must report to Archives all retention schedules applied to record series they maintain.[61]

Authority: Utah Code §§ 63A-12-103, 112, 113, 63G-2-604, and Utah Adminstrative Code R36-1-1 *et seq.*

2.5 **Record Series Privacy Annotation**

State agencies are required to perform privacy annotations[62] for each record series that contains personal data, pursuant to Utah Code § 63A-19-401.1 and additional requirements to be provided via administrative rulemaking.[63] The annotation process ensures agencies track, by record series, the legal authority for processing personal data, the purposes and uses for the personal data, and the types of personal data that may be processed in a specific record series. This tracking helps ensure proper data governance and risk management occur.

Authority: Utah Code §§ 63A-19-301 and 401.1

2.6 **Inventorying**

Inventory of Processing Systems.
Under the Division of Technology Services (DTS) Information Security Policy 5000-0002[64], state agencies are required to maintain an inventory of all IT systems that may process state or federal data owned by or for which the State is responsible. This inventory must be consistent with NIST[65] Special Publications 800-53 Rev5 and use the standard process provided by DTS. An inventory of all systems that may process state data is necessary to ensure all systems are reasonably accounted for. Agencies can also use this inventory to ensure systems only process personal data for authorized purposes and that such processing remains necessary.

Inventory of Records Series and Personal Data.
As noted in Privacy Practice 2.5, state agencies are required to perform "privacy annotations" for each record series containing personal data.[66] One component of a complete privacy annotation is the inclusion of an inventory of the personal data within a particular record series.[67]

Inventory of Non-Compliant Processing Activities.
Governmental entities must, by no later than July 1, 2027, identify and document any non-compliant processing activity[68] that was implemented prior to May 7, 2025, and they must prepare a strategy for bringing them into compliance as soon as is reasonably practicable.[69] All processing activities implemented after May 7, 2025, must be compliant upon implementation.[70] [2]

Entities will then include information regarding processing activities implemented before May 7, 2025—as described inSubsections 63A19401(2)(a)(iv)(A) through (C)—in the privacy program report detailed in Section 63A-19-401.3.[71] The requirement to identify and document non-compliant processing activities implies—and thus it is recommended—that entities keep an inventory of all processing activities, not just the non-compliant ones.[72]

Authority: Utah Code §§ 63A-12-103, 104, 63A-19-401, and 401.1
Forthcoming administrative rule. DTS Information Security Policy 50000002[73]

2.7 **Privacy Impact Assessments (PIA)**

A privacy impact assessment (PIA) is a systematic process for analyzing how an IT system processes personal data. Its purpose is to ensure compliance with applicable privacy requirements and to identify and mitigate potential risks. The PIA serves as both an analytical process and a formal document detailing the methodology, findings, and outcomes of this analysis.

Under the DTS Information Security Policy 5000-0002, all state agencies must complete a PIA for any IT system that processes or will process personal data. This assessment must be completed *before* any data processing begins.[74] The CPO is responsible for creating and maintaining a standardized PIA template, which must be approved by the Chief Information Officer (CIO).[75] PIA templates are available at privacy.utah.gov or by contacting the Office.

Although Utah law does not currently mandate a standalone PIA, Utah Administrative Code R895-8-8 requires state agencies to complete a "Privacy Risk Assessment" for all online applications.[76] "Privacy Risk Assessment" is defined as:

- A series of questions approved by the CIO.
- Designed to help agencies identify and reduce privacy risks for individuals using online government services.
- Used to determine appropriate security levels.
- Intended to collect information needed to create an agency privacy policy.[77]

Additionally, state agencies are prohibited from collecting user data on a governmental website unless the site complies with a website privacy notice as required by Utah Code § 63A-19-402.5.

As such, agencies should complete a Privacy Risk Assessment *before* collecting user data on their websites. A copy of each completed assessment must be retained for four years for audit purposes.[78]

Authority: Utah Code §§ 63A-12-103, 104, 63A-19-401, and 401.1
Forthcoming administrative rule. DTS Information Security Policy 50000002[73]

2.8 **Record and Personal Data Sharing, Selling, or Purchasing**

Under the GDPA, a governmental entity must have the appropriate legal authority to share personal data and is prohibited from selling[79] personal data unless expressly required by law.[80] An entity may be authorized to share records containing personal data under various GRAMA provisions. This is distinct from public records requests or data subject access requests.[81] GRAMA provisions may allow data to be shared with other governmental entities, contractors, private providers, or for research purposes.[82] GRAMA details specific requirements and restrictions based on the parties, purpose, and the types of data (records) involved. However, GRAMA's sharing provisions do not apply to all records, as other more specific laws may take precedence.[83] Entities and their legal counsel must account for these many variables when analyzing data sharing. The following sections outline some of the most common legal bases for sharing, though entities are responsible for knowing and applying all applicable laws.

Legal Basis for Sharing Records with Other Governmental Entities

Utah Code § 63G-2-206(1), (2), and (3) provide three separate legal bases for sharing records with other governmental entities.[84]

Legal Basis for Sharing Records for Research Purposes

Utah Code § 63G-2-202(8) provides requirements and restrictions for disclosing private or controlled records for research. Entities must analyze the governing law for appropriate applicability, as numerous code sections specifically address data disclosure for research.

Legal Basis for Sharing Records with Contractors and Private Providers

GRAMA, at Subsection 63G-2-206(6), provides the requirements and restrictions for disclosing records containing personal data to contractors and private providers. The GDPA adds new requirements for these relationships:

- A contractor that processes or has access to personal data is subject to the GDPA to the same extent as the governmental entity.[85]
- A contract entered into or renewed after July 1, 2026, must include specific language requiring the contractor to comply with GDPA requirements.[86]
- These GDPA requirements for contractors are in addition to any other applicable law or liability.[87]
- Contractors are not subject to the GDPA's privacy training requirements.[88]

Other Legal Bases for Sharing Records

Entities are responsible for knowing the legal bases (e.g., state and federal law) they may use to share non-public records that may contain personal data.

Contracts that Involve Personal Data

Governmental entities must ensure contracts that involve personal data include appropriate privacy protection terms and conditions. It is best practice to consult with legal counsel to ensure compliance with the many different state and federal laws, regulations, policies, and contractual obligations that may apply to particular data, entities, or programs. Such requirements may include those mandated by the Division of Purchasing and General Services or by DTS with respect to IT-related agreements.[89] Examples of privacy protecting terms and conditions can be found at privacy.utah.gov or by contacting the Office.

Reporting Data Sharing, Selling, or Purchasing

As noted in Privacy Practice 1.5, the annual privacy program report must include the following information as required by Utah Code § 63A-19-401:

- A list of the types of personal data shared, sold, or purchased;[90]
- The legal basis for these activities.
- The categories of individuals or entities with whom the data is shared, sold, or purchased.

Agreements for Data Sharing

Although a written agreement is not always legally required for sharing personal data, it is considered best practice. Legal counsel should be consulted to determine when a written agreement is necessary and to ensure that all privacy and personal data provisions are adequately addressed.[91]

It is important to remember that government records are statutorily established as property owned by the state.[92] Misuse by entity employees can trigger both criminal and civil penalties.[93] Thus, it is imperative that governmental entities work closely with their legal counsel to

ensure that personal data contained in government records is shared in compliance with applicable laws, rules, and other privacy requirements. Data sharing agreement templates can be found at privacy.utah.gov or by contacting the Office.

Authority: Utah Code §§ 63A-19-401, 401.4, 63G-2-202, and 206

CONTROL

3.1 **Data Subject Requests for Access**

GRAMA provides that, "if access to records is governed by a more specific court rule or order, state statute, federal statute, or federal regulation prohibits or requires sharing information, that rule, order, statute, or federal regulation controls."[94] If a record is only governed by GRAMA, then the act details specific circumstances under which a person may access it (e.g., Utah Code § 63G-2-202 *Access to private, controlled, and protected documents*). When a governmental entity provides private or public records about an individual, as specified in Subsection 63G-2-202(1), it must also disclose the context in which the record is used upon request.[95] Archives is statutorily mandated to prepare forms for all governmental entities to use when a person requests access to a record.[96]

Additionally, Utah Code § 63A-19-402.5 requires a governmental entity's website privacy notice to include a method for an individual to seek access to their personal data or user data.[97] Political subdivisions may adopt a jurisdiction-wide ordinance or policy for information practices, including record access, denials, and appeals.[98] Such an ordinance or policy must establish access criteria, procedures, response times, and time limits for appeals consistent with GRAMA.[99] If a political subdivision does not adopt and maintain such an ordinance or policy, then that entity is subject to the provisions of GRAMA.[100]

Authority: Utah Code §§ 63A-19-402.5, 63G-2-202, and 206

3.2 **Data Subject Requests for Amendment or Correction**

GRAMA requires entities to allow individuals to contest the accuracy or completeness of any public, private, or protected record concerning them by requesting the governmental entity amend the record pursuant to the strictures detailed in Utah Code § 63G-2-603. Proceedings of a governmental entity in this respect are also governed by Title 63G, Chapter 4, Administrative Procedures Act.[101]

- If the entity approves the request, it must correct all of its records containing the same incorrect information and may not disclose the record until it has been amended.[102]
- If the entity denies the request, the requester may submit a written statement contesting the information in the record.[103] The entity must file the statement with the disputed record such that the statement can accompany the record or make the statement accessible.[104] The entity must disclose the statement along with the information in the record whenever it discloses the disputed information.[105]
- The right to request an amendment does not apply to records relating to title to real property, medical records, judicial case files, or other records that the entity determines must be maintained in their original form to protect the public interest and to preserve the integrity of the record system.[106]

Political subdivisions may adopt a jurisdiction-wide ordinance or policy for information practices, including amendment of records.[107] If adopted, each ordinance or policy must establish criteria, procedures, and response times for requests to amend records, and time limits for appeals consistent with GRAMA.[108] If a political subdivision does not adopt and maintain such an ordinance or policy, then that entity is subject to the provisions of GRAMA.[109] Additionally, Utah Code § 63A-19-402.5 requires a governmental entity's website privacy notice to include a method for an individual to request an amendment or correction of their personal data furnished to the entity.[110]

A governmental entity that collects personal data must have a procedure by which an individual or legal guardian may request an amendment or correction of personal data furnished to the governmental entity.[111] Amendment and correction of personal data by a governmental entity, and the procedure by which an individual makes such a request, must comply with all applicable laws and regulations to which the personal data and the governmental entity are subject (e.g., GRAMA).[112] Having a procedure for individuals to request an amendment or correction does not obligate the entity to make the requested amendment or correction.[113]

Authority: Utah Code §§ 63A-19-402.5, 403, 63G-2-603, and 701

3.3 **Data Subject Requests for an Explanation**

An individual asked by a governmental entity to furnish information that could be classified as a private or controlled record may request from the governmental entity, and the entity must explain to the individual:

- The reasons the person is asked to furnish the information.
- The intended uses of the information.
- The consequences for refusing to provide the information.
- The reasons and circumstances under which the information may be shared with or provided to other persons or governmental entities.[114]

A governmental entity must, upon request, provide the personal data collection privacy notice required in Utah Code § 63A-19-402 to an individual or legal guardian regarding personal data they previously furnished to the governmental entity.[115]

Authority: Utah Code §§ 63A-19-402 and 63G-2-601

3.4 **Data Subject Request by At-Risk Employees for Restricting Access**

Utah Code § 63G-2-303 requires governmental entities to create and maintain a form for at-risk government employees.[116] This form allows them to file a written application to have records containing their personal information[117] classified as private. Applicants using this form may request assistance from the governmental entity to identify individual records that fall within the scope of their request. A submitted form remains in effect for four years, even if the employee's employment ends. It also remains in effect for one year after the entity receives official notice of the employee's death, or until the employee rescinds the form.[118]

The requirements of Section 63G-2-303 are detailed and cover everything from the form's content to the necessary actions and procedures that must be part of the process. As a result, entities and their legal counsel must carefully analyze the law to ensure compliance.

Furthermore, Utah Code § 63A-19-402.5 mandates that a governmental entity's website privacy notice include a way for at-risk employees to request their personal information be classified as a private record under Section 63G-2-302.[119]

Authority: Utah Code §§ 63A-19-402.5 and 63G-2-303

COMMUNICATE

4.1 **Privacy Notice (Notice to Provider of Information)**

Governmental entities must provide a privacy notice to individuals or their legal guardians about when collecting personal data.[120] The specific requirements for this notice depend on the governing law:

- GDPA: Entities subject to the GDPA must provide a privacy notice when requesting or collecting personal data from an individual.
- GRAMA Part 6: Entities subject to GRAMA's notice requirements must provide a notice to any person asked to furnish personal data that could be classified as a private or controlled record.[121]
- Other law: Entities may be subject to notice requirements in other superseding or preempting laws and regulations.

Due to the legal complexity, legal counsel should be consulted to determine which law applies to a particular entity and to ensure compliance. In general, a privacy notice is a written statement that informs a person about how an entity will collect, use, and share their personal data. An entity should not collect personal data without complying with either Subsection 63G-2-601(2) or Section 63A-19-402, as appropriate.

Under Subsection 63G-2-601(2), the notice must include:

- The record series that will contain the information.
- The reasons for collecting the information.
- The intended uses of the information.
- The consequences for refusing to provide the information.
- The classes of persons and the governmental entities that share information with or receive information from the entity on a regular or contractual basis.

Additionally, the notice must be posted in a prominent place where the information is collected or included directly in the documents or forms used to collect the information.

Under Utah Code § 63A-19-402, a governmental entity must provide a privacy notice when collecting personal data. The content of the notice depends on whether the data is a public record.

- If the personal data is a public record:[122] The entity needs to provide a privacy notice with a statement indicating that the individual's personal data may be available to the public as provided by Section 63G-2-201.[123]

If the personal data is *not* a public record:[124] The privacy notice must be more detailed, describing the following:

- The intended purposes and uses of the personal data.
- The consequences for refusing to provide the personal data.
- The record series in which the personal data is included.
- The classes of persons and governmental entities with whom the personal data is shared or to whom it is sold.[125]

A governmental entity must provide this privacy notice by one of the following methods:

- Posting it in a prominent place where the personal data is collected.
- Including it as part of any document or form used to collect the personal data.
- Including a conspicuous link or QR code to an electronic version of the notice as part of any document or form used to collect the personal data.[126]

An important element of the GDPA not addressed in GRAMA is the provision for processing activities that serve a public safety interest or produce a public benefit greater than or equal to the potential impact on an individual's privacy.[127] Examples include:

- The provision of emergency services.
- Law enforcement body or dash camera recordings.
- Security camera monitoring.
- Ambulance and emergency medical services.
- 911 emergency communications.[128]

In such cases, the governmental entity may provide the privacy notice by posting it on the entity's website, or on the public notice website if the entity does not have a website.[129]

The notice required under Section 63A-19-402 is in addition to, and does not supersede, any other applicable notice.[130] A governmental entity is prohibited from using personal data for any purposes not identified in the privacy notice.[131] Additionally, upon request, an entity must provide the privacy notice to an individual, or their legal guardian, regarding personal data previously furnished by that individual.[132] Privacy notice templates are available at privacy.utah.gov or by contacting the Office.

Some of the notice requirements of GRAMA are redundant with provisions of the GDPA. The Office is working with the Legislature to consolidate them appropriately within the GDPA.

Authority: Utah Code §§ 63A-19-402 and 63G-2-601

4.2 **Website Privacy Notice and Website Privacy Policy**

To promote transparency and public trust, governmental entities must comply with specific requirements for website privacy notices on government websites.[133] These notices ensure users can make informed decisions about their personal data.

As outlined in Utah Code § 63A-19-402.5, governmental entities must include a privacy notice on any website that collects user data. State agencies must also adhere to Utah Admin. Code R895-8, which details requirements related to the Privacy Policy Statement For State of Utah Websites and its relationship with a state agency privacy policy, where applicable.

A governmental entity may not collect user data on its websites unless it has a website privacy notice that includes:

- The identity of the governmental entity responsible for the website and how to contact them.
- A method for a user to:
  - Seek access to their personal data or user data.
  - Request to correct or amend their personal data or user data.
  - File a complaint with the data privacy ombudsperson.
- Instructions for at-risk employees to request that their personal information be classified as a private record under Section 63G-2-302.

If the website collects user data, the privacy notice must also provide details on:

- Any website tracking technology used.
- What user data is collected.
- The intended purposes and uses of the user data.
- The record series in which the user data is included.
- The classes of persons and governmental entities with whom the user data is shared or sold.

A website privacy notice must be prominently posted on the homepage of the government website or accessible via a link on the homepage. User data may not be collected unless the website privacy notice requirements are met. Website privacy notice templates are available at privacy.utah.gov or by contacting the Office.

The requirements for the Privacy Policy Statement For State of Utah Websites are redundant with provisions of the GDPA. The Office is working with appropriate governmental entities to consolidate them appropriately within the GDPA.

Authority: Utah Code § 63A-19-402.5 and Utah Admin. Code 895-8

PROTECT

5.1 **Minimum Data Necessary**

Entities must obtain and process only the minimum amount of personal data necessary to efficiently achieve a specified purpose.

Authority: Utah Code § 63A-19-401

5.2 **Retention and Disposition of Records Containing Personal Data**

Pursuant to Utah Code § 63G-2-604(1)(b), entities are required to maintain, archive, and dispose of records in accordance with an approved retention schedule. For more details on retention schedules, their approval process, and entity applicability, refer to Privacy Practice 2.3 of this Framework.

Further, Utah Code § 63A-19-404 requires governmental entities that collect personal data to retain and dispose of it in accordance with a documented record retention schedule.[135] Governmental entities must comply with all other applicable laws or regulations related to retention or disposition of personal data they hold.[136]

Authority: Utah Code §§ 63A-19-404 and 63G-2-604

5.3 **Incident Response and Notification to the Cyber Center and Attorney General**

Governmental entities are subject to specific requirements for responding to and reporting data breaches. The Office coordinates with the Cyber Center[137] to develop an incident response plan for data breaches[138] affecting governmental entities.[139] The Cyber Center is charged with providing incident response capabilities to state agencies and, upon request, coordinating cybersecurity incident response for a data breach affecting other governmental entities.[140] The DTS Cybersecurity Incident Response Plan outlines the general procedures for all state agencies when responding to a data breach or security incident.

Notification for Breaches Affecting 500 or More Individuals

Under Utah Code § 63A-19-405, a governmental entity must notify the Cyber Center and the State Attorney General's Office of a data breach affecting 500 or more individuals. This notification must be made without unreasonable delay and no later that five days from the discovery of the breach.[141]

The notification must include the following information:

- The total number of individuals affected.
- The types of personal data involved.
- The date and time the breach occurred.
- The date the breach was discovered.
- A short description of the breach.
- The means by which access was gained to the system, computer, or network.
- The person who perpetrated the breach.
- The steps the entity takes to mitigate the impact.
- Any other details requested by the Cyber Center.[142]

If the required information is not available within five days, the entity must provide as much available information as possible and supplement the notification as additional details become available.[143]

Internal Reporting for Breaches Affecting Fewer Than 500 Individuals

For data breaches affecting fewer than 500 individuals, entities must create and report an internal incident report in accordance with Subsection 63A-19-405(5). Upon request, the entity must provide this internal report to the Cyber Center, as well as an annual report logging all data breaches affecting fewer than 500 individuals.[144]

Additional Reporting and Compliance

Beyond the data breach notifications detailed above, a governmental entity that identifies unauthorized access, acquisition, disclosure, loss of access, or destruction of data that compromises the security, confidentiality, availability, or integrity of its computer systems or information maintained must also notify the Cyber Center in the manner it prescribes.[145] For non-IT incidents, such as unauthorized access to physical records, an entity may be required to have an entity-specific incident response plan.

These data breach notification requirements are in addition to any other applicable reporting requirements to which the entity may be subject to (e.g., the Health Insurance Portability and Accountability Act (HIPAA)).[146] Entities should consult with their legal counsel to analyze and determine the applicability and precedence of all relevant reporting requirements.

Authority: Utah Code § 63A-19-405 and Cyber Security Incident Response Plan

5.4 **Breach Notification to Affected Individuals**

Breach Notice to Individuals Affected by a Data Breach

Under Utah Code § 63A-19-406, a governmental entity must provide a data breach notice to an individual, or their legal guardian, if the individual's personal data is affected.[147] The notice is to be provided after the entity determines the scope of the data breach and restores the reasonable integrity of the affected system, and without unreasonable delay.[148] An entity must delay providing the notice if a law enforcement agency requests it.[149]

Content of Individual Data Breach Notice

The data breach notice to an individual must include:

- A description of the breach.
- The individual's personal data that was or may have been accessed.
- Steps the entity is taking to mitigate the impact of the breach.
- Recommendations on how to protect against identity theft and other financial losses.
- Any other language required by the Cyber Center.

Breach notification templates are available at privacy.utah.gov or by contacting the Office.

Methods of Providing Notice to Individuals

With some exceptions, the entity must provide the data breach notice to an individual by email or mail and provide a summary of the notice and instructions for accessing the full notice by text or telephone message.[150] When a data breach affects more than 500 individuals and the governmental entity cannot obtain an individual's contact information, the entity must provide notice in a manner reasonably calculated to have the best chance of being received. This may include a press release, appropriate social media accounts, or publishing a notice in a newspaper of general circulation.[151]

Exception to Individual Notice Requirement

A governmental entity is not required to provide individual notice of a data breach if the breached personal data would be classified as a public record under Utah Code § 63G-2-301 and the entity prominently posts a notice on its website homepage.[152]

Coordination with Other Laws

Governmental entities that are currently subject to other breach notification requirements (e.g., HIPAA, 42 CFR Part 2, FERPA), are required to create and maintain their own entity-specific policies and procedures that meet the requirements of the applicable regulations.

Authority: Utah Code § 63A-19-406

PART 2: PRIVACY MATURITY AND STRATEGIES

PRIVACY MATURITY MODEL

The privacy maturity model is a practical framework designed to help governmental entities effectively assess and improve the maturity of their privacy practices. Higher maturity levels not only strengthen privacy protections but also clearly demonstrate a proactive commitment to continuous improvement. While a low maturity level may meet basic compliance requirements, it often indicates a program that is not reasonably continuous or active, which can significantly increase. The heightened risk can stem from issues such as inadequate documentation, overreliance on individual knowledge, or a lack of institutionalization, making the program vulnerable to disruptions like staff turnover.

The privacy maturity model serves as a foundational tool for entities to:

- Based on the maturity assessment, determine strategies that will increase the maturity of specific privacy practices.
- Identify a target maturity level that the entity aims to achieve upon successful implementation of strategies.
- Document any identified strategies in the annual privacy program report.

ENTITY STRATEGIES

Governmental entities are required to maintain continuous and active records management programs, which must incorporate privacy practices. To build an effective and resilient program, entities should use the privacy maturity model to identify specific opportunities for improvement. Based on these assessments, they can create and document tailored strategies—specific, actionable steps designed to enhance their privacy practices. This process of active self-assessment and strategic implementation allows entities to build effective and continuously improving privacy programs that can adapt to evolving challenges and requirements.[153]

When completed, individual maturity models for each identified privacy practice will be made available at **privacy.utah.gov** or by contacting the Office.

PRIVACY MATURITY MODEL

5 — OPTIMIZED
The practice is fully embedded in the entity with recognition and understanding across the workforce through active training and awareness campaigns, and inclusion in operations and strategy.

4 — MANAGED
The practice is actively managed with metrics that are reviewed to assess efficacy and facilitate improvement.

3 — CONSISTENTLY IMPLEMENTED
The practice is documented to cover all relevant aspects, application is formal and consistent.

2 — DEFINED
The practice is implemented and documented, but documentation may not cover all relevant aspects, and application may be informal and inconsistent.

1 — AD HOC
The practice may occur but is undocumented (no policies or procedures), application is reactive and not standardized.

0 — NON-EXISTENT
The practice is not implemented or acknowledged.

READY, SET, GO APPENDIX

By December 31, 2025, entities must have initiated their data privacy program. Entities may fulfill this obligation by completing their annual privacy program report by December 31, 2025, and then annually thereafter.[154] When using this Framework as the basis of a privacy program, the Office recommends that entities follow the phases of a simplified "ready, set, go" model, adapted from the NIST Privacy Framework.[155] This approach provides a clear order of operations for creating a new privacy program or maturing an existing one. While an entity is not required to use this model, the Office has included it in this Framework to serve as a helpful resource to guide them through the process. If an entity decides not to follow it, they will need to establish their own systematic approach for their privacy program.

READY

PREPARATION PHASE

1. Designate Responsibility

- Identify and designate an executive-level individual (Chief Administrative Officer (CAO)[156] or a designee) to be responsible for implementing the entity's data privacy program.[157]
- The CAO must appoint one or more records officers or other employees to implement and maintain the data privacy program and its practices.
- The CAO of each governmental entity is required to prepare an annual privacy program report.

SET

PLANNING & ASSESSMENT PHASE

2. Define Program Scope

- Outline the entity's privacy practices to align with both general and entity specific privacy requirements.
- Formalize the data privacy program with a policy, rule, ordinance, or other documentation that details its privacy practices.
- Document whether the entity has initiated a privacy program and any implemented privacy practices in the annual privacy program report.

3. Conduct Maturity Assessment

- Conduct an initial self-assessment using the privacy maturity model to measure the current maturity level of the entity's privacy practices.

4. Identify Strategies

- Based on the maturity assessment, determine strategies that will increase the maturity of specific privacy practices.
- Identify a target maturity level that the entity aims to achieve upon successful implementation of strategies.
- Document any identified strategies in the annual privacy program report.

5. Identify and Prioritize High-Risk Processing Activities

- Based on the maturity assessment, determine strategies that will increase the maturity of specific privacy practices.
- Identify a target maturity level that the entity aims to achieve upon successful implementation of strategies.
- Document any identified strategies in the annual privacy program report.

6. Identify Personal Data Sharing, Selling, or Purchasing

- Create an inventory of the types of personal data the entity shares, sells, or purchases, along with the legal basis for these activities.
- Create a list of the categories of individuals or entities with whom the data is shared, sold, or from whom it is purchased.
- Document both the inventory and the list in the entity's annual privacy program report.

GO

EXECUTION & MONITORING PHASE

7. Implement Prioritized Strategies

- Implement identified strategies to mature the entity's privacy practices.
- After implementing each strategy, update the maturity assessment to reflect the new status of the practice. Creating and prioritizing new strategies should be continuous to further advance privacy maturity.

8. Utilize Privacy Impact Assessments (PIA)

- Use the Office's Privacy Impact Assessment to evaluate new processing activities before implementation to ensure compliance with the GDPA and other applicable privacy requirements.

9. Privacy Awareness Training

- Require all employees to complete the privacy awareness training provided by the Office or an equivalent training created by the entity and approved by the Office.
- Document the percentage of employees who have fulfilled the privacy training requirements in the entity's annual privacy program report.

PATH FORWARD

The Office aims to support entities in initiating their data privacy programs and maturing their privacy practices. The Office anticipates that additional legislative changes will occur to improve privacy laws and move Utah toward alignment with the State Data Privacy Policy[158] in future General Sessions. The practices and efforts outlined in this Framework will be revisited and updated as a new version when appropriate.

Looking forward, the Office views the initiative to increase the maturity of data privacy programs and practices across governmental entities as an ongoing commitment that will involve consistent effort to ensure the privacy programs of governmental entities effectively protect the privacy interests and rights of individuals.

ENDNOTES

[1] Utah Code § 63A-19-101 *et seq.*

[2] Utah Code § 63A-19-401(2)(a)(i).

[3] Utah Code § 63A-19-301(3)(a).

[4] This iteration of the Framework Version 2.0 (V2.0) finalized 09/11/2025.

[5] "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).

[6] Cybersecurity duties and obligations are not addressed in this Framework.

[7] During the 2024 General Session the Legislature enacted HB491, known as the GDPA, which is codified at Title 63A, Chapter 19.

[8] See Utah Code § 63G-2-701 for applicability of GRAMA to political subdivisions.

[9] See Utah Code § 63A-19-103(26).

[10] Utah Code § 63A-19-102.

[11] See Utah Code § 63A-19-401(1)(b).

[12] Utah Code § 63A-12-103.

[13] Utah Code § 63A-12-103(8)(c).

[14] Utah Code § 63A-12-103(9).

[15] Utah Code § 63A-12-103(1).

[16] Utah Code § 63A-12-103(4).

[17] Utah Code § 63A-12-103(4).

[18] "Records officer" 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(27).

[19] Utah Code § 63A-12103(2).

[20] Utah Code § 63A-12-103(8)(c)(ii).

[21] Utah Code § 63G-2-108.

[22] Utah Code § 63A-19-301(3)(f).

[23] Utah Code § 63A-19-401.2(2).

[24] Utah Code § 63A-19-401.2(3).

[25] Utah Code § 63A-19-301(3)(g).

[26] Utah Code § 63A-19-401.2(1)(a)(i) and (ii).

[27] Utah Code § 63A-19-401.3(1)(a) and (b).

[28] Utah Code § 63A-19-401.3(1)(c)—(e).

[29] Utah Code § 63A-19-401.3(1)(f) and (g). See Utah Code § 401(2)(a)(iv)(A)—(D) for additional requirements on information to be included in the report.

[30] Utah Code § 63A-19-401.3(2)(a) and (b).

[31] Utah Code § 63A-19-401(2)(b).

[32] Utah Code § 63A-12-103(1). *See Deseret News Pub. Co. v. Salt Lake Cnty.*, 2008 UT 26, ¶¶ 13 and

15 stating that "GRAMA … strives to accomplish its legislative goals by creating a government records classification system and by requiring records management practices for state agencies."

[33] Utah Code § 63G-2-103(25).

[34] Utah Code § 63G-2-103(25).

[35] See Utah Code § 63G-2-103(26).

[36] See Utah Code §§ 63A-19-404, 63G-2-307, 604, and 701.

[37] Utah Code § 63G-2-307(1)(a)-(c) (See Utah Code 63A-12-103(8)(a) and (b)).

[38] Utah Code § 63G-2-103(8)

[39] Utah Code § 63G-2-103(4).

[40] Utah Code § 63G-2-307(1)(a)-(c) and (2). (See Utah Code § 63A-12-103(2)&(8)) (See *S. Utah Wilderness All. v. Automated Geographic Reference Ctr., Div. of Info. Tech.*, 2008 UT 88, ¶ 17) (See *also*, *Deseret News Pub. Co. v. Salt Lake County*, 182 P.3d 372 (Utah 2008) primary classification as an alternative to a designation).

[41] Utah Code § 63G-2-701(2)(a).

[42] Utah Code § 63G-2-701(2)(b), (3)(a) and (b).

[43] Utah Code § 63G-2-701(2)(c).

[44] Utah Code § 63G-2-701(2)(f).

[45] Utah Code § 63G-2-601(1)(a).

[46] Utah Code § 63G-2-601(1)(b)(i).

[47] Utah Code § 63G-2-601(1)(b)(ii).

[48] Utah Code § 63G-2-601(4).

[49] "Schedule," "scheduling," and their derivative forms mean the process of specifying the length of time each record series should be retained by a governmental entity for administrative, legal, fiscal, or historical purposes and when each record series should be transferred to the state archives or destroyed. Utah Code § 63G-2-103(28)."

[50] Utah Code § 63G-2-604(1)(b).

[51] Utah Code § 63A-12-103(10).

[52] Utah Code §§ 63A-12-103(5) and 63G-2-604(1)(a).

[53] Utah Code § 63G-2-604(1)(b).

[54] Utah Code § 63G-2-604(1)(c).

[55] Utah Code § 63A-12-101(2)(e).

[56] Utah Code § 63A-12-113(1)(b).

[57] https://archives.utah.gov/rmc/index.html

[58] Utah Code § 63G-2-701(2)(a).

[59] Utah Code § 63G-2-701(2)(b) and (3)(d).

[60] Utah Code § 63G-2-701(2)(c).

[61] Utah Code § 63G-2-701(2)(f).

[62] "Privacy annotation" means a summary of personal data contained in a record series as described in Section 63A-19-401.1. Utah Code § 63A-19-101(25).

[63] Utah Code § 63A-19-301(4)(f).

[64] DTS Information Security Policy 5000-0002, section 2.4.2.1.

[65] National Institute of Standards and Technology (NIST)

[66] Utah Code § 63A-19-401.1.

[67] Utah Code § 63A-19-401.1(2)(b)(i).

[68] "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).

[69] Utah Code § 63A-19-401(2)(a)(iv)(A), (B), and (C).

[70] Utah Code § 63A-19-401(2)(a)(iii) and (iv).

[71] Utah Code § 63A-19-401(2)(a)(iv)(D).

[72] Utah Code § 63A-19-401(2)(a).

[73] https://services.dts.utah.gov/esc?id=kb_article&sysparm_article=KB0010265

[74] DTS Information Security Policy 5000-0002 section 2.4.3.1 Privacy Impact Assessments.

[75] *Id.*

[76] Utah Administrative Code R895-8-8.

[77] Utah Administrative Code R895-8-4(9).

[78] UT ADC R895-8-8.

[79] Utah Code § 63A-19-101(33).

(33) (a) "Sell" means an exchange of personal data for monetary consideration by a governmental entity to a third party.

(b) "Sell does not include a fee:

(i) charged by a governmental entity for access to a record pursuant to Section 63G-2-203; or

(ii) assessed in accordance with an approved fee schedule.

[80] See Utah Code § 63A-19-401(3)(b) and (c).

[81] See Utah Code § 63G-2-206.

[82] See Utah Code § 63G-2-202(8) sharing for research.

[83] See Utah Code § 63G-2-206(7).

[84] This is not meant to suggest that the three stated provisions are the only provisions of GRAMA that may be applicable.

[85] Utah Code § 63A-19-401.4(1).

[86] Utah Code § 63A-19-401.4(2).

[87] Utah Code § 63A-19-401.4(3).

[88] Utah Code § 63A-19-401.4(4).

[89] https://purchasing.utah.gov/forms/.

[90] "Purchase" or "purchasing" means the exchange of monetary consideration to obtain the personal data of an individual who is not a party to the transaction. Utah Code § 63A-19-101(29).

[91] See Utah Code § 63A-19-401.4.

[92] Utah Code § 63A-12-105.

[93] See Utah Code §§ 63A-12-105, 63A-19-602, 63G-2-801, and 63G-2-804.

[94] Utah Code § 63G-2-206(7).
[95] Utah Code § 63G-2-602.
[96] Utah Code 63A-12-101(2)(l).
[97] Utah Code 63A-19-402.5(1)(c)(i).
[98] Utah Code § 63G-2-701(2)(a).
[99] Utah Code § 63G-2-701(2)(b) and (3)(d).
[100] Utah Code § 63G-2-701(2)(c).
[101] Utah Code § 63G-2-603(1).
[102] Utah Code § 63G-2-603(4).
[103] Utah Code § 63G-2-603(6)(a).
[104] Utah Code § 63G-2-603(6)(b)(i).
[105] Utah Code § 63G-2-603(6)(b)(ii).
[106] Utah Code § 63G-2-603(8).
[107] Utah Code § 63G-2-701(2)(a).
[108] Utah Code § 63G-2-701(2)(b) and (3)(d).
[109] Utah Code § 63G-2-701(2)(c).
[110] Utah Code § 63A-19-402.5(1)(c)(ii).
[111] Utah Code § 63A-9-403(1).
[112] Utah Code § 63A-19-403(2).
[113] Utah Code § 63A-19-403(3).
[114] Utah Code § 63G-2-601(2)(a) and (3)(a)—(d).
[115] Utah Code § 63A-19-402(6).
[116] "At-risk government employee" is a defined term at Utah Code § 63G-2-303(1)(a) for use in Section 63G-2-303.
[117] "Personal information" is a defined term at Utah Code § 63G-2-303(1)(c) for use in Section 63G-2303.
[118] Utah Code § 63G-2-303(6).
[119] Utah Code § 63A-19-402.5(1)(d).
[120] Utah Code § 63A-19-402(1).
[121] Utah Code § 63G-2-601(2).
[122] See Utah Code § 63G-2-301 (classification of public records).
[123] Utah Code § 63A-19-402(2)(a).
[124] See Utah Code § 63G-2-301 (classification of public records).
[125] Utah Code § 63A-19-402(2)(b).
[126] Utah Code § 63A-19-402(3).
[127] Utah Code § 63A-19-402(5)(a)(i)—(ii).
[128] Utah Code § 63A-19-402(5)(b).
[129] Utah Code § 63A-19-402(5)(a).
[130] Utah Code § 63A-19-402(4).
[131] Utah Code § 63A-19-402(7).

[132] Utah Code § 63A-19-402(6).

[133] Utah Code § 63A-19-101(16):

(16) “Government website” means a set of related web pages that is operated by or on behalf of a governmental entity and is:

(a) located under a single domain name or web address; and

(b) accessible directly through the internet or by the use of a software program.

[134] Utah Code § 63A-19-401(2)(a)(ii).

[135] Utah Code § 63A-19-404(1).

[136] Utah Code § 63A-19-404(2).

[137] Utah Code § 63A-16-1102.

[138] “Data breach” means the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by a governmental entity, unless the governmental entity concludes, according to standards established by the Cyber Center, that there is a low probability that personal data has been compromised. Utah Code § 63A-19-101(11).

[139] Utah Code § 63A-19-301(3)(e).

[140] Utah Code § 63A-16-1102(4)(b) and (c)

[141] Utah Code § 63A-19-405(2)(a).

[142] Utah Code § 63A-19-405(2) and (3).

[143] Utah Code § 63A-19-405(4).

[144] Utah Code § 63A-19-405(5).

[145] Utah Code § 63A-19-405(1)(b).

[146] See Utah Code § 63A-19-401(1).

[147] Utah Code § 63A-19-401(2)(b).

[148] Utah Code § 63A-19-406(1)(a).

[149] Utah Code § 63A-19-406(2).

[150] Utah Code § 63A-19-406(4).

[151] Utah Code § 63A-19-406(5).

[152] Utah Code § 63A-19-406(1)(b).

[153] Utah Code § 63A-12-103.

[154] Utah Code § 63A-19-401.3.

[155] https://www.nist.gov/privacy-framework.

[156] Utah Code § 63A-12-100.5(2)(a).

[157] Utah Code § 63A-12-103.

[158] Utah Code § 63A-19-102.