

STATE OF UTAH

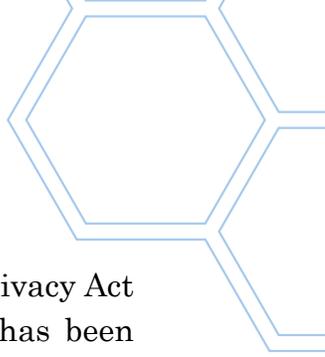
Office of Data Privacy



Privacy Program Framework

Version 1.0





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. The Office is directed to—among other things—assist state agencies in meeting their privacy obligations.

Under the GDPA a state agency is required to have a privacy program—that includes the agency's policies, practices, and procedures for the processing of personal data—implemented by May 1, 2025. This Privacy Program Framework (Framework) is provided to agencies by the Office, in part, as a resource to assist agencies in meeting the May 1, 2025, deadline. It is anticipated that there will be other versions of the Framework as the content is refined and revised with stakeholder feedback, as new and amended laws dictate, and potentially with iterations that are specific to particular governmental entities. The Office will create and maintain tools, training, and other resources that align with this Framework. Please contact the Office with any feedback or questions that your entity may have with respect to this Framework.

What is a Privacy Program?

A privacy program is the structured collection of an agency's privacy practices, policies, and procedures that govern its processing and protection of personal data to ensure compliance with applicable laws. A privacy program will likely meet the May 1, 2025, deadline even if it is in its early stages. This Framework is a blueprint that agencies may adopt as a foundational part of their program. The Framework consists of privacy practices based on legal requirements, a maturity model for measuring the maturity of practices to inform an agency’s strategies to improve maturity, and efforts of the Office to assist agencies with their privacy obligations.

This approach aligns with the May 1, 2025, requirement by providing a roadmap for agencies to establish, at a minimum, an initial privacy program. Over time, agencies can increase the maturity of their privacy program, while taking into account their available resources, the current maturity of their privacy practices, and their goals for advancing operational complexity, effectiveness, and understanding.

Privacy Program Framework

Laws

This Framework is aligned with Utah law and administrative rules that are generally applicable across state agencies with respect to implementing appropriate privacy

practices. All state agencies are required to have a privacy program with adequate privacy practices that also account for agency specific laws or regulations, including governing federal laws and regulations.

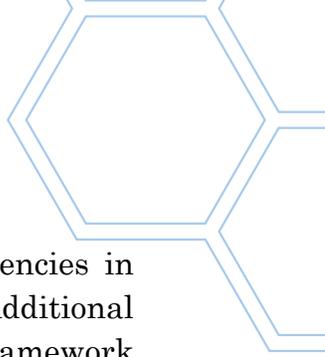
Privacy Practices

This Framework includes 21 privacy practices identified by the Office based on its analysis and interpretation of generally applicable Utah law and administrative rule. Summary analysis and description of each practice, along with legal basis and available tools and resources associated with the practice can be found in Part 1 of this Framework and on <https://privacy.utah.gov>.

Privacy Maturity Model and Strategies

This Framework includes a standard maturity model that may be used by agencies to measure the maturity of the privacy practices of their privacy program. Based on their assessments, agencies should then develop and document tailored strategies the agency will implement over time to increase the maturity of their practices and program. Additional information about the privacy maturity model can be found in Part 2 of this Framework. Individual maturity models for each identified privacy practice can be found on <https://privacy.utah.gov>.

Level	Description
Level 0 Non-Existent	The practice is not implemented or acknowledged.
Level 1 Ad Hoc	The practice may occur but is undocumented (no policies or procedures), application is reactive and not standardized.
Level 2 Defined	The practice is implemented and documented, but documentation may not cover all relevant aspects, and application may be informal and inconsistent.
Level 3 Consistently Implemented	The practice is documented to cover all relevant aspects, application is formal and consistent.
Level 4 Managed	The practice is actively managed with metrics that are regularly reviewed to assess efficacy and facilitate improvement.
Level 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.



Efforts of the Office of Data Privacy

This Framework includes specific efforts of the Office to assist state agencies in meeting their privacy obligations and maturing their privacy practices. Additional information about the efforts of the Office can be found in Part 3 of this Framework and on <https://privacy.utah.gov>.

Next Steps: Ready, Set, Go!

By May 1, 2025, agencies must have implemented their privacy program. The Office recommends that agencies that are initiating a new program or those that are maturing an existing program use a simple model of “ready, set, go” phases that have been adapted from the NIST Privacy Framework.¹

Ready: Preparation Phase

1. Designate Responsibility:

- o Identify who at the executive level (CAO or designated individual) will be responsible for implementing the agency's privacy program.
- o The CAO must also appoint one or more records officers, or other specified employees, who will be responsible for implementing and maintaining aspects of the agency's privacy program and associated practices.

Set: Planning and Assessment Phase

2. Define Program Scope:

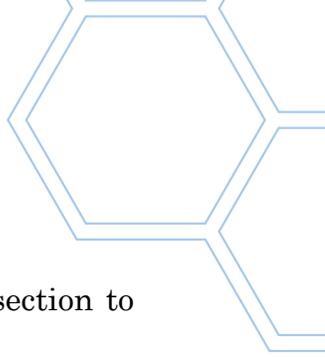
- o Outline the agency's specific privacy practices to ensure alignment with both generally applicable and agency-specific privacy requirements.
- o Formalize the privacy program through an adopted policy, rule, or other documentation that explicitly defines the adopted privacy practices.

3. Conduct Maturity Assessment:

- o Use the privacy maturity model to perform an initial self-assessment to measure the current maturity level of the agency's privacy practices.

4. Identify and Prioritize Strategies:

- o Based on the maturity assessment, determine and prioritize strategies that the agency plans to effectuate to increase the maturity of specific privacy practices. This should include setting a target maturity level for one or more practices that the agency aims to achieve if a specific strategy is implemented successfully.



Go: Execution and Monitoring Phase

5. Implement Prioritized Strategies:

- o Execute the prioritized strategies identified in the previous section to mature the agency's privacy practices.
- o Following each strategy's implementation, update the maturity assessment to reflect the new status of the agency's privacy practices. Continuously create and prioritize new strategies to further advance privacy practice maturity.

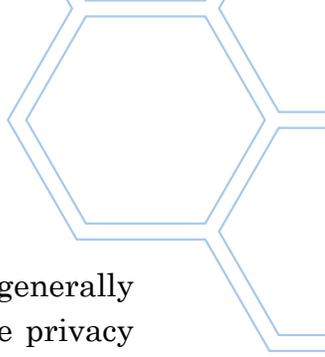
6. Utilize Privacy Impact Assessments (PIA):

- o Use the Privacy Impact Assessment the Office provides to evaluate new processing activities before implementation to ensure compliance with the GDPR and any other applicable privacy requirements.

Path Forward

The Office aims to support agencies in implementing their 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 Policy² in the 2025 and 2026 General Sessions. The practices and efforts outlined in this Framework will be revisited and updated as needed.

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



Introduction to the Framework

This Framework is aligned with Utah law and administrative rules that are generally applicable across state agencies with respect to implementing appropriate privacy practices. By May 1, 2025, all state agencies are expected to have a privacy program with adequate privacy practices that also account for agency specific laws or regulations, including governing federal laws and regulations.

Requirements for the privacy practices of state agencies are found in provisions of law spread throughout state and federal law and regulation. The Government Data Privacy Act³ (GDPA) is an initial step toward standardizing and consolidating privacy requirements for governmental entities to the greatest extent possible, but this will be an incremental process over the long-term.

As the long-term process unfolds, agencies remain generally subject to the 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 (DARS)—formerly known as the Public Records Management Act. Although these two acts are generally thought of as record management laws, they also contain privacy practices that overlap with records management practices, e.g., inventorying, classification, retention, and disposition. This allows agencies to align data privacy program policies and practices with the records management life cycle.

Agencies should be familiar with their current privacy obligations and available resources to assist with compliance. This Framework provides a high-level overview of those obligations as well as available resources via the Office as follows:

Part 1: Privacy Practices

Current state agency privacy obligations are outlined with associated guidance.

Part 2: Privacy Maturity Model and Strategies

A standard model for use by agencies and the Office for internal self-assessment and measurement of privacy practice maturity to inform policy, strategy, and risk management recommendations and decisions.

Part 3: Efforts of the Office of Data Privacy

Information about the Office and its strategies to assist agencies to increase the maturity of their privacy practices.

Part 1: Privacy Practices

Privacy Practices.

For purposes of this Framework, *privacy practices*, generally refers to administrative, physical, and technical safeguards that agencies must implement and adhere to in order to safeguard personal data, comply with legal duties, and ensure individuals are advised of their rights with respect to their personal data. Agencies are responsible for ensuring their privacy practices adequately protect individual’s privacy, adhere to the State Data Privacy Policy⁴, comply with applicable privacy related laws, regulations, and policies, and allow the agency to carry out its mandates. The following privacy practices, listed below, are foundational to privacy programs and are meant to ensure that agencies are adequately protecting individuals’ privacy. Agencies are required to account for these practices in their privacy program unless subject to a more specific or preempting law.

Practice Category	Practice #	Privacy Practice Name
Govern	1	Chief Administrative Officer Designation
	2	Records Officers Appointment
Record Series	3	Record Series Creation and Maintenance
	4	Record Series Designation and Classification
	5	Retention Schedule Proposal and Approval
Awareness and Training	6	Record Series Privacy Annotation
	7	Records Officers Training and Certification
Identify	8	Statewide Privacy Awareness Training
	9	Inventorying
Transparency	10	Privacy Impact Assessment
	11	Website Privacy Policy
Processing	12	Privacy Notice (Notice to Provider of Information)
	13	Minimum Data Necessary
	14	Record and Data Sharing or Selling
Information Security	15	Record Retention and Disposition
	16	Incident Response
Individual Requests	17	Breach Notification
	18	Data Subject Requests for Access
	19	Data Subject Requests for Amendment or Correction
	20	Data Subject Requests for an Explanation
	21	Data Subject Request At-Risk Employee Restrictions

Chief Administrative Officer (CAO) DesignationAuthority: [Utah Code § 63A-12-103](#)

Agencies are required to designate one or more CAOs. Agencies are also asked to report the designation to Archives. The CAO of each state agency is mandated to establish and maintain an active, continuing program for the economical and efficient management of the agency's records as provided by DARS and GRAMA.⁵ Additionally, the CAO is responsible for creating and maintaining adequate and proper documentation of the organization, functions, policies, decisions, procedures, and essential transactions of the agency designed to furnish information to protect the legal and financial rights of persons directly affected by the agency's activities.⁶ An agency's designated CAO is primarily responsible for the creation and maintenance of policies and procedures associated with the privacy practices identified in this Framework.

Records Officers AppointmentAuthority: [Utah Code § 63A-12-103\(2\)](#)

Agency CAOs are required to appoint one or more records officers who are responsible for ensuring the “care, maintenance, scheduling, disposal, classification, designation, access, and preservation of records.”⁷ The records officer is responsible for following policies and procedures created by the CAO which are associated with the privacy practices identified in this Framework.

Record Series Creation and MaintenanceAuthority: [Utah Code §§ 63G-2-103\(25\) and 26](#), and [63A-12-103](#).

State agencies manage and maintain records according to the requirements of GRAMA. 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 state agency (and where all of the information in the original is reproducible by photocopy or other mechanical or electronic means and is not explicitly provided in GRAMA as not being a “record”).⁸ State agencies then group records that may be treated as a unit for purposes of designation, description, management, or disposition into “records series.”⁹ Records must be maintained according to their record series attributes, e.g., retention, classification, and purpose and use limitations.

Record Series and Record Designation and Classification

Authority: [Utah Code §§ 63G-2-103](#) and [307](#).

Record and record series designation and classification are governed by both GRAMA and DARS, which require state agencies to evaluate and designate each record series that the agency keeps, uses, or creates and to report the designation and privacy annotation to DARS.¹⁰ GRAMA provides distinct definitions of both designation and classification at Utah Code § 63G-2-103(7) and (3) respectively.

GRAMA defines designation to mean “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.”¹¹

GRAMA defines classification to mean “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).”¹²

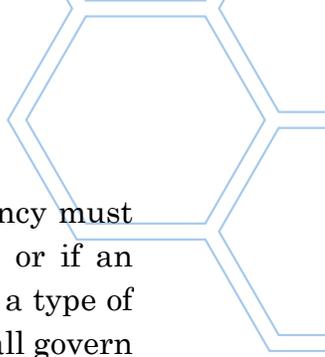
Thus, although an agency is not required to classify a particular record, record series, or information until access to the record is requested, per Utah Code § 63G-2-307(2), the statute still requires designation of record series irrespective of whether a request has been made or not.¹³

Retention Schedule Proposal and Approval

Authority: Utah Code §§ [63A-12-103](#), [63A-12-112](#), [63A-12-113](#), [63G-2-604](#), and [Utah Administrative Code R36-1-1 et seq.](#)

The Records Management Committee (RMC)¹⁴ is responsible for reviewing and approving retention schedules for governmental entities. Agencies are required to submit and obtain approval for record series retention schedules from the RMC according to the procedures outlined in [Utah Administrative Code R36-1](#).

The CAO of a state agency 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 for final approval by the RMC.¹⁵ The RMC is responsible for reviewing and determining whether to approve each schedule for the retention and disposal of records and must do so within three months after the day on which the proposed schedule is submitted to the committee.¹⁶



After a retention schedule is reviewed and approved by the RMC, the agency must maintain and destroy records in accordance with the retention schedule or if an agency has not received an approved retention schedule from the RMC for a type of record, the general retention schedule maintained by the state archivist shall govern the retention and destruction. The procedures for RMC meetings and retention 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 [website of the Division of Archives and Records Service](#).¹⁷

Privacy Practice 6

Record Series Privacy Annotation

Authority: [Utah Code §§ 63A-12-104](#) and [63A-12-115](#).

Forthcoming administrative rule.

State agencies are required to perform “privacy annotations” for each record series that contains personal data pursuant to Utah Code § 63A-12-115 and additional requirements that will be provided via administrative rulemaking.¹⁸ The annotation is a process that is meant to ensure that agencies track, by record series, the legal authority under which they process 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 to ensure proper risk management occurs.

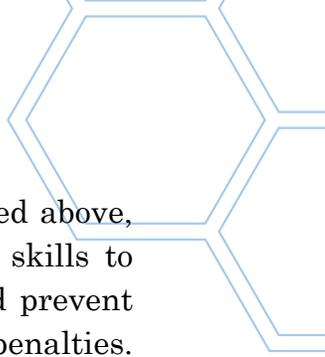
Privacy Practices 7 and 8

Privacy Awareness and Training

Authority: [Utah Code §§ 63G-2-108](#) and [63A-19-301\(5\)](#).

Privacy awareness training educates employees about privacy laws, regulations, best practices, internal policies, and employee responsibilities. The training ensures employees have the knowledge and skills to handle personal data appropriately, recognize and respond to privacy concerns, promote early detection and prevention of privacy incidents, and reduce data breach risks. Overall, privacy training and awareness programs build a privacy-conscious workforce. The following are required awareness and training requirements for state agencies:

Privacy Practice 7: Appointed Records Officer Training: Each records officer of an agency must, on an annual basis, successfully complete online training on the provisions of GRAMA and obtain certification from Archives in accordance with Section 63A-12-110.¹⁹ AROs have the responsibility to implement many of the practices identified in this Framework.



Privacy Practice 8: Statewide Privacy Awareness Training: As noted above, privacy awareness training ensures employees have the knowledge and skills to appropriately handle PII, recognize and respond to privacy concerns, and prevent privacy incidents, thus reducing the risk of data breaches and potential penalties. Employees of state agencies that have access to personal data as part of the employee's work duties are required to complete a data privacy training program within 30 days after beginning employment and at least once in each calendar year.²⁰

Privacy Practice 9

Inventorying

Authority: [Utah Code §§ 63A-12-103, 63A-12-104, and 63A-19-401](#). Forthcoming administrative rule. DTS Information Security Policy 5000-0002.²¹

Inventory of Processing Systems.

Under the Division of Technology Services (DTS) Information Security Policy 5000-0002, section 2.4.2.1, state agencies are required to maintain an inventory of all IT systems that may process state or federal data which the State owns or is responsible for, consistent with National Institute of Standards and Technology, Special Publications 800-53 Rev5, using the standard process that DTS provides. An inventory of all systems that may process state data is necessary to ensure that all systems are reasonably accounted for. Agencies may then also use this inventory to ensure that systems only process personal data for authorized purposes and that the processing is still necessary for the authorized purposes.

Inventory of Records Series and Personal Data.

As noted in Privacy Practice #6, state agencies are required to perform “privacy annotations” for each record series that contains personal data pursuant.²² One of the requirements for performing a privacy annotation is the inclusion of an inventory of the personal data that is included in the particular record series.²³

Inventory of Non-Compliant Processing Activities.

State agencies must comply with the requirements in Utah Code § 63A-19-401, which includes a requirement to identify and document any non-compliant processing activity that was implemented prior to May 1, 2024, and prepare a strategy for bringing the non-compliant processing activity into compliance no later than January 1, 2027.²⁴ All processing activities implemented after May 1, 2024, must be compliant as of implementation. This documenting requirement implies, and thus it is recommended, that agencies keep an inventory of all processing activities not only those that are non-compliant.²⁵

Privacy Impact Assessments (PIA)

Authority: Utah Code § 63A-12 -103(4) and Utah Admin R895-8, DTS Information Security Policy 5000-0002.

A privacy impact assessment (PIA) is an analysis of how personally identifiable information is processed in a system to ensure that processing conforms with applicable privacy requirements and assists in identifying privacy risks that may need to be mitigated. A PIA is both an analysis and a formal document that details the process and outcome of the analysis. Under DTS Information Security Policy 5000-0002, state agencies are required to complete a PIA for all IT systems that may process personal data prior to processing personal data in the IT system.²⁶ Pursuant to the DTS Information Security Policy the CPO will create and maintain a standard privacy impact assessment template that is approved by the Chief Information Officer.²⁷

Although Utah law may not explicitly require completion of a PIA, administrative rule does require state agencies to complete a “Privacy Risk Assessment” for all online applications.²⁸ Privacy Risk Assessment is defined to mean: “... a series of questions approved by the Chief Information Officer that are designed to:

- (a) assist agencies in identifying and reducing potential levels of risk to the privacy of individuals using an online government service through state of Utah Websites;
- (b) provide information to assist in determining different levels of security;
- (c) collect information needed to determine, and if necessary, create an agency privacy policy if one is needed in addition to the State Policy.”²⁹

Additionally, a state agency may not collect personal data related to a user of the agency's governmental website unless the agency has taken reasonable steps to ensure that on the day on which the personal data is collected the agency's governmental website complies with a compliant privacy policy statement in accordance with Utah Code § 63D-2-103. As such, agencies should complete a Privacy Risk Assessment prior to collection of personal data on an agency's website. The agency must maintain a copy of each completed assessment for four years to provide audit documentation.³⁰

Website Privacy Policy

Authority: Utah Code § 63D-2-103 and Utah Admin. Code 895-8.

Agencies are required to create and maintain privacy policies on their websites as outlined in Utah Code § 63D-2-103 and Utah Admin. Code R895-8. Clearly stating an agency's data practices and privacy commitments allows users to make informed decisions about sharing their personal data. A well-crafted privacy policy helps build public confidence by demonstrating value and respect for privacy.

A state agency may not collect personal data related to a user of the agency's website unless the governmental entity has taken reasonable steps to ensure that on the day the personal data is collected, the governmental entity's website complies with Utah Code § 63D-2-103(2), which states:

A governmental website shall contain a privacy policy statement that discloses:

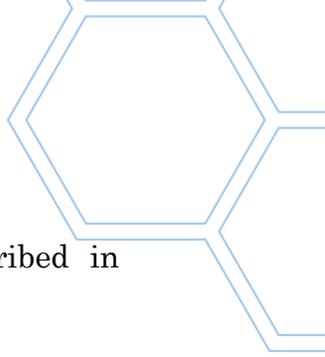
- The identity of the governmental website operator;
- How the governmental website operator may be contacted;
- The personal data collected by the governmental entity;
- The practices related to disclosure of personal data collected by the governmental entity and/or the governmental website operator; and
- The procedures, if any, by which a user of a governmental entity may request:
 - Access to the user's personal data; and
 - Access to correct the user's personal data.
- A general description of the security measures in place to protect a user's personal data from unintended disclosure.

Privacy Notice (Notice to Provider of Information)

Authority: Utah Code §§ 63G-2-601(2), 63D-2-103(2)-(3), and 63A-19-402.

Agencies are required to provide a notice to persons that are asked to furnish personal data to an agency.³¹ A privacy notice is a written statement that informs persons about how an agency will be collect, use, and share their personal data. An agency should not collect personal data from persons unless the agency has taken reasonable steps to ensure that on the day the personal data is collected, the agency complies with Subsection 63G-2-601(2), which provides:

An executive branch agency shall provide the notice described in Subsection (2) to a person that is asked to furnish personal data.

- 
- The notice required under Subsection (2)(b) shall:
 - Identify the **record series** that includes the information described in Subsection (2)(b);
 - State the **reasons** the person is asked to furnish the information;
 - State the **intended uses** of the information;
 - State the **consequences for refusing** to provide the information; and
 - Disclose the classes of persons and the governmental entities that currently:
 - Share the information with the governmental entity; or
 - Receive the information from the governmental entity on a regular or contractual basis.

And, the governmental entity shall:

- Post the notice required under this Subsection (2) in a prominent place at all locations where the governmental entity collects the information; or
- Include the notice required ... as part of the documents or forms that are used by the governmental entity to collect the information.

Pursuant to Utah Code § 63A-19-402 governmental entities are required to provide a personal data request notice to an individual, or the legal guardian of an individual, from whom the entity requests or collects personal data. Elements that must be included in the notice are detailed in Subsection (2) and requirements on providing and posting the notice are detailed in Subsection (3). The personal data request notice required under Section 402 is in addition to, and does not supersede, any other notice requirement that is otherwise applicable to a governmental entity. Governmental entities are restricted from using personal data furnished by an individual for any purposes that were not identified in the personal data request notice.

Privacy Practice 13

Minimum Data Necessary

Authority: Utah Code § 63A-19-401(2)(c).

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

Record and Data Sharing or Selling

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

State agencies must have appropriate legal authority to share or disclose personal data.³² Agencies may not sell personal data unless expressly required by law.³³ Agencies may share records that contain personal data under specific record management provisions of GRAMA—this is distinct from access requests for public records or access requests of a data subject which are each discussed elsewhere in this Framework.³⁴ Such sharing may be to a distinct component or program within an agency, or may be to another governmental entity, contractor, private provider, or researcher.³⁵ GRAMA details requirements and restrictions that are applicable depending on the parties, purposes, and the records (data) involved. However, sharing provisions of GRAMA may not apply to all records as GRAMA contemplates that other specific laws may pre-empt the data sharing provisions of GRAMA. There are many aspects that must be accounted for by an agency and its legal counsel whenever data sharing is being analyzed.

Legal Basis for Sharing Records with Other Government Entities

Utah Code § 63G-2-206(1), (2), and (3) contain three separate legal bases that a state agency may use when sharing records with other governmental entities.

Legal Basis for Sharing Records for Research Purposes

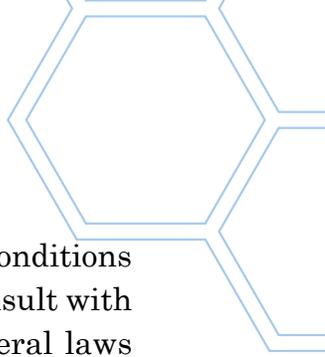
Utah Code § 63G-2-202(8) provides requirements and restrictions under which an agency may disclose private or controlled records for research purposes.

Legal Basis for Sharing Records with Contractors and Private Providers

Utah Code § 63G-2-206(6) provides requirements and restrictions under which an agency may disclose records that contain personal data with contractors and private providers. Utah Code § 63A-19-401(4) adds new requirements to contractors that enter into or renew an agreement with a governmental entity that deals with processing or access to personal data after May 1, 2024.

Other Legal Bases for Sharing Records

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



Contracts that Involve Personal Data

State agencies must ensure that appropriate privacy protection terms and conditions are included in contracts that involve personal data. It is best practice to consult with legal counsel to ensure compliance with the many different state and federal laws and regulations, policies, and contractual obligations that may apply to particular data, agencies, 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.³⁶

Reporting Data Sharing or Selling

State agencies must annually report to the CPO the types of personal data the agency currently shares or sells³⁷, the basis for sharing or selling, and the classes of persons and governmental entities that receive the personal data from the agency.³⁸

Agreements for Data Sharing

Although there is not always a requirement that sharing of personal data be addressed in a written agreement, it is best practice to do so. Legal counsel will need to verify when a written agreement is needed as well as that data sharing provisions involving privacy and personal data are adequately addressed.³⁹

It is important to remember that government records are statutorily established as property that is owned by the state.⁴⁰ Misuse by agency employees can trigger both criminal and civil penalties.⁴¹ Thus, it is imperative that state agencies work closely with legal counsel to ensure that personal data contained in government records is shared in compliance with applicable laws, rules, and other privacy requirements.

Privacy Practice 15

Retention and Disposition of Records Containing Personal Data

Authority: [Utah Code §§ 63G-2-604\(1\)\(b\) and 63A-19-404.](#)

Pursuant to Utah Code § 63G-2-604(1)(b) agencies are required to maintain, archive, and dispose of records in accordance with the approved retention schedule.

Further, Utah Code § 63A-19-404 requires governmental entities that collect personal data to retain and dispose of the personal data in accordance with a documented record retention schedule. Governmental entities must comply with all other applicable laws or regulations related to retention or disposition of specific personal data held by that governmental entity.

Incident Response

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

Agencies are required to appropriately safeguard the personal data in their possession. The DTS Cybersecurity Incident Response Plan informs all agencies, employees, and contractors of the State of Utah of their obligation to protect personal data and establishes procedures for responding to a breach or incident.

Incident response refers to the systematic approach taken by an agency to address and manage security incidents or data breaches. It involves a series of actions, including detection, containment, eradication, recovery, and post-incident analysis. Incident response is vital as part of a privacy plan for several reasons:

- Incident response minimizes the impact of security incidents and mitigates potential harm to individuals' privacy.
- Incident response helps agencies comply with regulatory requirements that mandate the implementation of incident response capabilities.
- Incident response enables agencies to learn from incidents, identify vulnerabilities, and make improvements to prevent future occurrences.

Agencies are required to report all suspected incidents of any severity to the Enterprise Information Security Office (EISO).

For non-IT related incidents, such as unauthorized access of physical records, agencies may be required to have an agency specific incident response plan.

Notification to the Cyber Center and Office of the Utah Attorney General

Agencies are required to notify the Cyber Center and the state attorney general's office of a data breach affecting 500 or more individuals in accordance with Utah Code § 63A-19-405. Agencies that experience a data breach affecting fewer than 500 individuals must create and report an internal incident report in accordance with Subsection 63A-19-405(5). These requirements are in addition to any other reporting requirement that the agency may be subject to.

Breach Notification

Authority: Utah Code § 63A-19-406.

Breach Notice to Individuals Affected by Data Breach

Agencies are required to provide notice to an individual or the legal guardian of an individual, if the individual's personal data is affected by a data breach in accordance with Utah Code § 63A-19-406.⁴² State agencies that are currently subject to breach notification requirements, such as those required for compliance with federal regulations, laws or other governing requirements (HIPAA, 42 CFR Part 2, FERPA, etc.) are currently required to create and maintain their own agency specific breach notification policies and procedures that meet the requirements of the applicable regulations.

Data Subject Requests for Access

Authority: Utah Code §§ 63G-2-202(1)(a) and 63G-2-206(7).

GRAMA states 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."⁴³ If a record is only governed by GRAMA, then GRAMA details specific circumstances under which a person may access a record. Utah Code § 63A-12-101(2)(l) provides that Archives shall prepare forms for use by all governmental entities for a person requesting access to a record.

Utah Code § 63D-2-103 requires that the Privacy Policy of state websites on which personal information is collected include the procedures, if any, that a person may follow to request access to their personal information that may be collected by the agency.

Data Subject Requests for Amendment or Correction

Authority: Utah Code §§ 63G-2-603 and 63A-19-403.

GRAMA provides a means for persons to contest the accuracy of an agency record. Agencies are required to allow persons to contest the accuracy or completeness of any public, private, or protected record concerning them by requesting the governmental entity amend the record as required in Utah Code § 63G-2-603. Proceedings of a state agency in this respect are also governed by Title 63G, Chapter 4, Administrative Procedures Act.

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

Utah Code § 63D-2-103 requires that the privacy policy of state websites on which personal data is collected include the procedures, if any, that a person may follow to request a correction to the personal information that may be collected by the agency.

A governmental entity that collects personal data must allow an individual or legal guardian to request an amendment or correction of personal data that has been furnished to the governmental entity. Amendment and correction of personal data by a governmental entity must comply with all applicable laws and regulations to which the personal data at issue and to which the governmental entity is subject, e.g., GRAMA.⁴⁴

Data Subject Requests for an Explanation

Authority: Utah Code §§ 63G-2-601(3) and 63A-19-402(2).

Agencies must respond to requests for explanations about processing of the personal information of data subjects. Pursuant to Utah Code § 63G-2-601(3)(a)-(d), a person that is 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 governmental entity shall explain to the person:

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

A governmental entity shall, upon request, provide personal data request notice required in Utah Code § 63A-19-402(2) to an individual or legal guardian, regarding personal data they previously furnished to the governmental entity.⁴⁵

Data Subject Request by At-Risk Employees for Restricting Access

Authority: Utah Code § 63G-2-303.

Agencies are required to create and maintain a form that can be used by at-risk government employees to file a written application requesting the agency to classify, as private, records that would disclose the employee's personal information. Applicants may request assistance from agencies to identify individual records containing personal information that may be within the scope of the request.

Section 303 provides many detailed requirements which necessitate careful analysis by an agency to ensure compliance. Section 303 contains specific requirements for the content of the form and agency actions that must be part of the process established under the section.

Part 2: Privacy Maturity and Strategies

Privacy Maturity Model

The privacy maturity model enables agencies to assess the maturity of their privacy practices. This assessment is a crucial step toward continuous improvement within their privacy programs. While agencies may comply with certain privacy requirements even at low maturity levels, striving for higher maturity strengthens privacy protections.

The purpose of this model is to provide a basis for agencies to:

1. Assess their privacy practices and program.
2. Identify areas for improvement; and
3. Create strategies to affect the improvement and increase practice maturity.

Individual maturity models for each identified privacy practice will be made available at <https://privacy.utah.gov>.

Agency Strategies

Each agency must maintain a continuous and active records management program which should include practices that account for privacy considerations. For most practices, achieving a "Consistently Implemented" maturity level is likely a reasonable benchmark for an adequately mature privacy program. Lower maturity levels may indicate that a program is not reasonably continuous and active, which may increase risk due to situations such as inadequate documentation, operationalization, or turnover of key personnel.

Agencies should use the privacy maturity models to identify opportunities for improvement in specific practices. Based on their assessments and identified opportunities for improvement, agencies should then develop and document tailored strategies the agency may implement over time to increase the maturity of those practices. These strategies are specific actions designed to improve their privacy practices. By actively engaging with the privacy maturity model, conducting thorough assessments, identifying opportunities for improvement, and implementing appropriate strategies, agencies can cultivate effective and continuously improving privacy programs.

Privacy Maturity Model

Level	Description
Level 0 Non-Existent	The practice is not implemented or acknowledged.
Level 1 Ad Hoc	The practice may occur but is undocumented (no policies or procedures), application is reactive and not standardized.
Level 2 Defined	The practice is implemented and documented, but documentation may not cover all relevant aspects, and application may be informal and inconsistent.
Level 3 Consistently Implemented	The practice is documented to cover all relevant aspects, application is formal and consistent.
Level 4 Managed	The practice is actively managed with metrics that are reviewed to assess efficacy and facilitate improvement.
Level 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.

Part 3: Efforts of the Office of Data Privacy

The Office will pursue various efforts as part of a holistic approach to assist state agencies with meeting their privacy obligations and maturing their privacy practices.

Each effort, shown below, independently, and collectively contributes to the Office’s mission of safeguarding the data privacy rights of individuals with regards to governmental entities by assisting state agencies to implement effective and efficient privacy practices using tools and systems that protect the privacy of individuals. Additionally, the Office will adopt an adaptive approach to its efforts, maintaining the flexibility to respond to changing dynamics and allowing teams to “learn by doing.” The Office expects its efforts will shift over time, based on the effectiveness and overall impacts of the Office’s activities and feedback from stakeholders.

Privacy Efforts	Description
-----------------	-------------

Privacy Program Policies	The Office will create privacy program policy templates to assist agencies with meeting the requirements of Utah Code § 63A-19-401(2)(a). The templates will likely include policies for records management, personal data collection and processing activities, data correction and amendment procedures, processing activity assessment, and incident response and breach notice.
Role Based Accountability	The Office will coordinate with agencies to implement a system for agencies to identify and track requisite role designations and appointments associated with the agency’s privacy program.
Record Series System Modernization	Archives, in conjunction with the Office, will implement a modernized record series management system. This system will allow agencies to manage their records series, associated tasks, and workflows, creating efficiencies for agencies and across state government. Examples of tasks and workflows include privacy annotations, record series and retention schedule approvals, and reporting the sale or sharing of personal data.
Privacy.Utah.Gov	The Office will build a privacy website to provide information and resources for agency use. The site may include education and training resources, forms to request

	training or ask questions, policy templates, ombuds dispute and mediation information, a calendar of privacy events, and information on the activities of the Utah Privacy Governing Board and Utah Privacy Commission.
General Privacy Training	General data privacy training materials will be created for use by all governmental entities to provide education to employees and contractors as required by Utah Code § 63A-19-401(2)(j). The Office will provide standard data privacy training in a digital format for use by all state agency employees.
Role based Training	The Office will provide regular workshops, training, and certification opportunities will be provided for agency employees based on specific roles and responsibilities.
Privacy Impact Assessments (PIA)	The Office will develop Privacy Impact Assessments for specific processing activities. Agencies can use these PIAs to identify risks and assist with mitigation strategies.
Processing Activity Inventory and Compliance Strategies	The Office will provide agencies with a system for inventorying their processing activities, assessing those activities for compliance, and documenting the strategies for achieving compliance. This will assist agencies with meeting the requirements of Utah Code § 63A-19-401(2)(e).
High-Risk Processing Activities	The Office will monitor prioritized, high-risk processing activities of state agencies. The Office may also provide agencies with expertise and assistance with these high-risk activities.

Endnotes.

¹ <https://www.nist.gov/privacy-framework>.

² Utah Code § 63A-19-102.

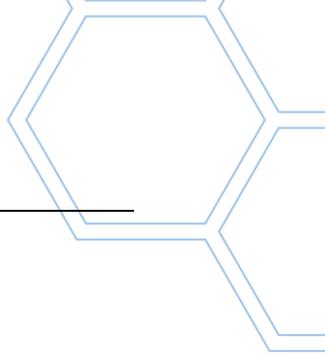
³ During the 2024 General Session the Legislature enacted HB491 as the GDPA, which will be codified at Title 63A, Chapter 19.

⁴ Utah Code § 63A-19-102.

⁵ Utah Code § 63A-12-103(1).

⁶ Utah Code § 63A-12-103(4).

⁷ Utah Code § 63A-12-103(2).

-
- 
- ⁸ See Utah Code § 63G-2-103(25).
- ⁹ See Utah Code § 63G-2-103(26).
- ¹⁰ Utah Code § 63G-2-307(1)(a)-(c) (See Utah Code 63A-12-115 privacy annotation).
- ¹¹ Utah Code § 63G-2-103(7)
- ¹² Utah Code § 63G-2-103(3).
- ¹³ Utah Code § 63G-2-307(1)(a)-(c) (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).
- ¹⁴ Utah Code § 63A-12-112
- ¹⁵ Utah Code §§ 63G-2-604(1)(a) and 63A-12-103(5).
- ¹⁶ Utah Code § 63A-12-113(1)(b).
- ¹⁷ <https://archives.utah.gov/rmc/index.html>
- ¹⁸ Utah Code § 63A-12-104.
- ¹⁹ Utah Code § 63G-2-108.
- ²⁰ Utah Code § 63A-19-301(5).
- ²¹ https://services.dts.utah.gov/esc?id=kb_article&sysparm_article=KB0010265
- ²² Utah Code § 63A-12-115
- ²³ Utah Code § 63A-12-115(2)(b)(i).
- ²⁴ "Process" or "processing" 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(14).
- ²⁵ Utah Code § 63A-19-401(2)(d) and (e).
- ²⁶ DTS Information Security Policy 5000-0002 section 2.4.3.1 Privacy Impact Assessments.
- ²⁷ *Id.*
- ²⁸ Utah Administrative Code R895-8-8.
- ²⁹ Utah Administrative Code R895-8-4(9).
- ³⁰ UT ADC R895-8-8.
- ³¹ Utah Code § 63G-2-601(2).
- ³² See Utah Code § 63A-19-401(2)(h).
- ³³ See Utah Code § 63A-19-401(2)(g).
- ³⁴ See Utah Code § 63G-2-206.
- ³⁵ See Utah Code § 63G-2-202(8) sharing for research.
- ³⁶ <https://purchasing.utah.gov/forms/>.
- ³⁷ "Sell" is a defined term at Utah Code § 63A-19-101(18).
- ³⁸ Utah Code § 63A-19-401(2)(i)(ii).
- ³⁹ See Utah Code § 63A-19-401(4)
- ⁴⁰ Utah Code § 63A-12-105.
- ⁴¹ Utah Code § 63G-2-801.
- ⁴² Utah Code § 63A-19-401(2)(b).
- ⁴³ Utah Code § 63G-2-206(7).
- ⁴⁴ Utah Code § 63A-19-403
- ⁴⁵ Utah Code § 63A-19-402(5).