Utah office of
Data Privacy

Presentation to Utah Privacy Commission

Christopher Bramwell
Chief Privacy Officer
November 12, 2025

State-Endorsed Digital Identity

- SEDI Summit occured Oct 17, 2025.
- https://www.uvu.edu/herbertinstitute/data_governance/state_endorsed_digital_identity_summit.html
- https://privacy.utah.gov/wp-content/uploads/SEDI_ProtectingLiberty.pdf

State-Endorsed Digital Identity

Jay Stanley • 1st
Speech, Privacy and Technology Project at American Civil Liberties Union (ACL...
2d •

Utah is embarked on an interesting, promising, and much-needed evaluation of digital identity, and what measures are needed to make sure it doesn't turn into a tracking nightmare.
https://lnkd.in/eNFnA9Mr

There's Only One State That is Asking the Right Questions About Digital Identity | ACLU
aclu.org

Privacy Program Framework

(3)The office shall:

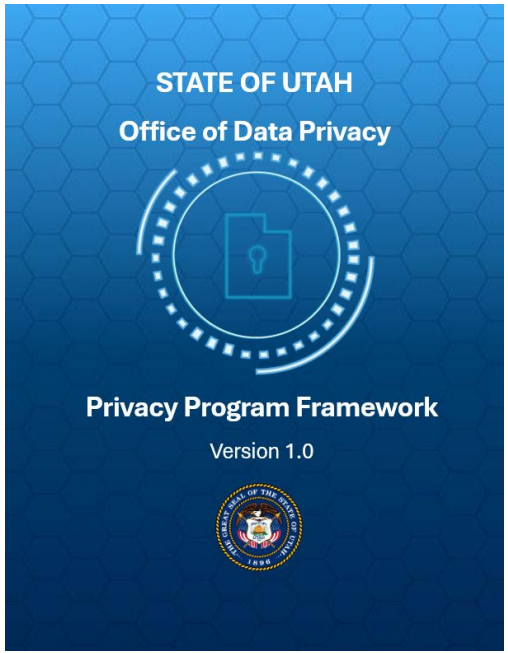
(a) create and maintain a data privacy framework designed to:
(i) assist governmental entities to identify and implement effective and efficient data privacy practices, tools, and systems that:
(A) protect the privacy of personal data;
(B) comply with data privacy laws and regulations specific to the governmental entity, program, or data;
(C) empower individuals to protect and control their personal data; and
(D) enable information use and sharing among governmental entities, as allowed by law; and
(E) account for differences in a governmental entity's resources, capabilities, populations served, data types, and maturity level regarding data privacy practices;

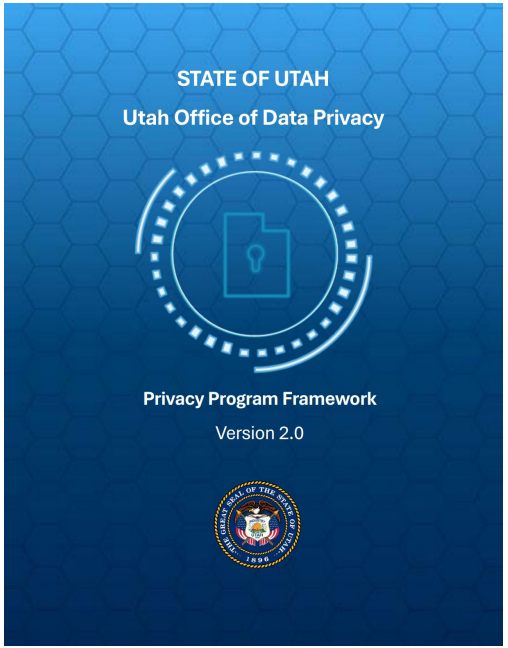
Privacy Program Framework

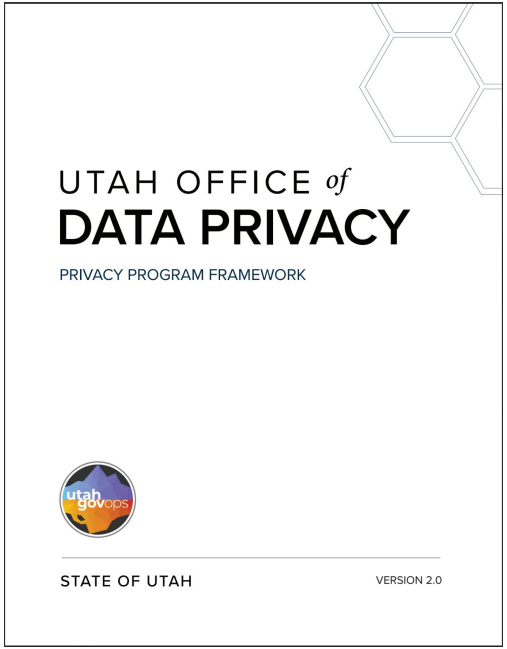
(1) The commission shall:

(b) develop guiding standards and best practices with respect to government privacy practices;

Privacy Program Framework







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 Gov-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.

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 Gov-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.

Practice Category	Practice Identifier	Privacy Practice Name
Govern	Gov-1.	Chief Administrative Officer (CAO) Designation 9
	Gov-2.	Records Officer Appointment 9
	Gov-3.	Records Officer Training and Certification 9
	Gov-4.	Statewide Privacy Training 10
	Gov-5.	Privacy Program Report 10
Identify	Ide-1.	Record Series Creation and Maintenance 11
	Ide-2.	Record and Record Series Designation and Classification 11
	Ide-3.	Statement Filed with State Archivist 12
	Ide-4.	Retention Schedule Proposal and Approval 13
	Ide-5.	Record Series Privacy Annotation 14
	Ide-6.	Inventorying 14
	Ide-7.	Privacy Impact Assessments (PIA) 15
	Ide-8.	Record and Personal Data Sharing, Selling, or Purchasing 16
Control	Con-1.	Data Subject Requests for Access 18
	Con-2.	Data Subject Requests for Amendment or Correction 18
	Con-3.	Data Subject Requests for an Explanation 19
	Con-4.	Data Subject Request by At-Risk Employees for Restricting Access 20
Communicate	Com-1.	Privacy Notice (Notice to Provider of Information) 20
	Com-2.	Website Privacy Notice and Website Privacy Policy 22
Protect	Pro-1.	Minimum Data Necessary 23
	Pro-2.	Retention and Disposition of Records Containing Personal Data 24
	Pro-3.	Incident Response and Notification to the Cyber Center and Attorney General 24
	Pro-4.	Breach Notification to Affected Individuals 25

CATEGORY	IDENTIFIER	PRIVACY PRACTICE NAMES
GOVERN	Gov-1	Chief Administrative Officer (CAO) Designation
	Gov-2	Records Officer Appointment
	Gov-3	Records Officer Training and Certification
	Gov-4	Statewide Privacy Training
	Gov-5	Privacy Program Report
IDENTIFY	Ide-1	Record Series Creation and Maintenance
	Ide-2	Record and Record Series Designation and Classification
	Ide-3	Inventorying
	Ide-4	Statement Filed with State Archivist
	Ide-5	Retention Schedule Proposal and Approval
	Ide-6	Record Series Privacy Annotation
	Ide-7	Privacy Impact Assessments (PIA)
	Ide-8	Record and Personal Data Sharing, Selling, and Purchasing
CONTROL	Con-1	Data Subject Requests for Access
	Con-2	Data Subject Requests for Amendment or Correction
	Con-3	Data Subject Requests for an Explanation
	Con-4	Data Subject Requests by At-Risk Employees for Restricting Access
COMMUNICATE	Com-1	Privacy Notice (Notice to Provider of Information)
	Com-2	Website Privacy Notice and Website Privacy Policy
PROTECT	Pro-1	Minimum Data Necessary
	Pro-2	Retention and Disposition of Records Containing Personal Data
	Pro-3	Incident Response and Notification to the Cyber Center and Attorney General
	Pro-4	Breach Notification to Affected Individuals

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.

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.

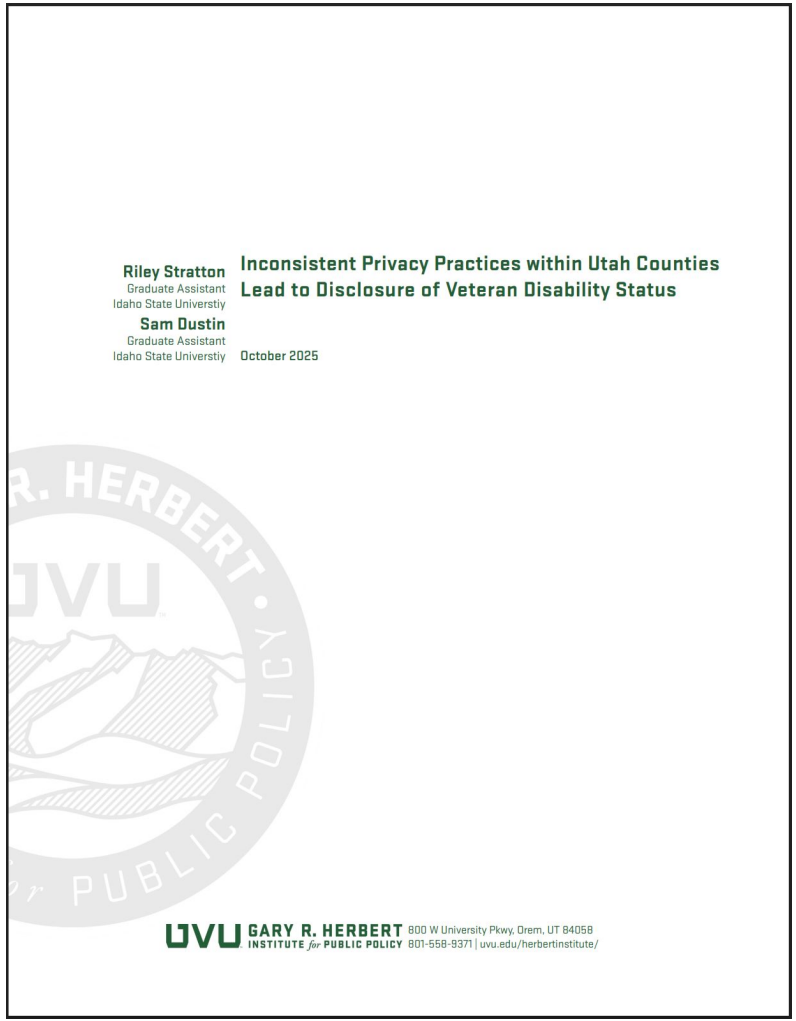
0 — NON-EXISTENT
The practice is not implemented or acknowledged.

5

Version 2.1 Privacy Program Framework changes in the works.

- Visual style and layout improvements
- Move “Ready, Set, Go” to an appendix.
- Add list and mapping of available tools and templates to appendix.

Discussion: Change privacy practice identifier structure from alphanumeric to just numeric. Gov-1 to 1.1, Ide-1 to 2.2, etc.



"This case study unequivocally demonstrates a critical gap in privacy protections across Utah's counties. The decentralized management of property tax records has resulted in an unequal application of privacy practices, where more than half of Utah's counties publicly disclose the disability status of resident veterans. While government transparency is important, it should not come at the cost of exposing sensitive personal data, especially when it concerns a population that warrants a high level of protection."

https://www.uvu.edu/herbertinstitute/docs/inconsistent_privacy_practices_within_utah_counties_leads_to_disclosure_of_veteran_disability_status.pdf

Legislation Discussion:

- Privacy commission's role in creating/maintaining broad consensus standards.

- Add members to commission to represent impacted categories of entities that have vested interest in adopting and maintaining standards to meet compliance requirements.