# The Current State of Data Governance in Utah

## Balancing Data Privacy, Transparency, and Use

February 2025

**William Freedman***
Research Assistant
**Grace Wingate***
Research Assistant
**Barclay Burns, PhD**
Assistant Dean,
School of Engineering
& Technology
Utah Valley University
**David R. Connelly, PhD**
Associate Provost, Student Success
Utah Valley University

*Equal contribution

UVU GARY R. HERBERT INSTITUTE for PUBLIC POLICY
800 W University Pkwy, Orem, UT 84058
801-558-9371 | uvu.edu/herbertinstitute/

# Executive Summary

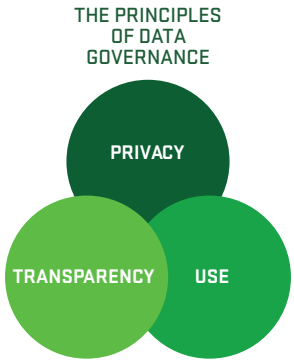
Effective data governance seeks to achieve the proper balance between protecting individuals' data privacy and promoting government transparency with how data is being used, while ensuring needed data can still be used effectively. It is an essential component of keeping the government accountable. This white paper examines the current state of data governance in Utah, reviewing its legal framework, operational challenges, and the benefits of having standardized data governance across all categories of governmental entities.

The Office of Data Privacy (ODP) has developed a Privacy Program Framework to assist governmental entities in developing privacy programs that comply with generally applicable laws. This white paper analyzes the Privacy Program Framework to provide insights on how it may help to modernize data governance.

In support of furthering data governance efforts, Utah Valley University's Smith College of Engineering and Technology is working to create a knowledge base of information generally applicable to data governance in Utah, including Utah code and statute. They are creating an AI model to inform users of the applicable requirements for managing data according to the law. This tool aims to enhance data governance, assist governmental entities in becoming compliant with data governance laws, and streamline information searches.

The UVU Herbert Institute plans to author subsequent white papers regarding Utah's efforts to modernize data governance and provide recommendations for future versions of the ODP's Privacy Program Framework. These papers will equip policymakers, governmental entities, and the public with the information needed to build a unified data governance framework.

The interviews cited throughout this white paper were conducted anonymously allowing respondents to provide information without impacting their role in government. Where publicly recorded, attribution of statements is sourced and identified, while statements provided during interviews have been included with the express consent of the interviewees. Any identifying information has been removed to protect their identities.




# Introduction to Data Governance and Current Legal Framework

Data governance is the framework of laws, rules, policies, practices, and procedures that ensure effective management, privacy, and transparency of data collected by governmental entities. The Legislature establishes in statute the requirements for transparency, privacy, and use of data. Implementation of data governance that reasonably balances transparency, privacy, and use of government-collected data according to the law is critical to maintaining public trust and accountability of governmental entities. Entities


may be subject to more specific or restrictive laws, but in the state of Utah, all governmental entities are subject to the following four generally applicable laws:

- The Government Records Access and Management Act (GRAMA),[1]
- The Division of Archives and Records Service and Management of Government Records (DARSMGR),[2]
- The Government Data and Privacy Act (GDPA),[3]
- The Government Internet Information Privacy Act (GIIPA).[4]

Entities may be subject to more specific or restrictive laws, but in the state of Utah, all governmental entites are subject to the following four generally applicable laws:

- The Government Records Access and Management Act (GRAMA)[1]
- The Division of Archives and Records Service and management of Government Records (DARSMGR)[2]
- The Government Data Privacy Act (GDPA)[3]
- The Government Internet Information Privacy Act (GIIPA)[4]

## GRAMA

GRAMA was enacted in 1991 and established Utah's foundational data governance practices. The primary purpose of the statute is to outline how citizens can request government records, which records are available, and how agencies retain records. The legislative intent behind GRAMA "recognizes two constitutional rights— the public's right of access to information concerning the conduct of the public's business; and the right of privacy in relation to personal data gathered by governmental entities."[5] Additionally, GRAMA aims to provide governmental entities with "fair and reasonable records management practices"[6] in order to ensure efficient data use.

GRAMA defines a record as a book, letter, document, paper, map, plan, photograph, film, card, tape, recording, electronic data, or other documentary material that is prepared, owned, received, or retained by a governmental entity or political subdivision. All data, including digital data in all modalities, unless specifically defined as not being a record, is subject to GRAMA requirements.[7] A governmental entity must classify and designate record series, which are used to categorize groups of related records that all share similar content or purposes such as marriage licenses, or election registrations. All records compiled by governmental entities are sorted into these record series.[8] To maximize efficiency, governmental entities should avoid commingling data between record series, and keep individual record series organized in all formats, both digital and physical.

## DARSMGR

DARSMGR establishes in code the authorities and responsibilities of the Division of Archives and Records Service (DARS). DARS is tasked with, "Administering the state's archives and records management programs."[9] Codified in 1969,[10] the code has gone through a series of revisions, the most recent amendments being in 2024.[11] DARSMGR is primarily focused on establishing generally applicable practices related to the management, preservation, retention, and disposal of records. The code also describes data governance roles specific individuals play within a governmental entity concerning records management.[12]

## GDPA

During the 2024 general session, the Utah State Legislature enacted GDPA. While GRAMA and DARSMGR define comprehensive government duties related to the right of transparency and use of data, GDPA is the first comprehensive law concerned primarily with privacy requirements applicable to governmental entities. GDPA established baseline privacy requirements for all Utah public entities unless an entity "is subject to a more restrictive or a more specific provision of law."[13] When asked about GDPA, one government official said, "GDPA is designed to create a baseline for a governmental entity's privacy obligations to its citizens."[14] It requires each governmental entity to implement a privacy program by May 1, 2025. Any processing activity that includes personal data implemented by a governmental entity after May 1, 2024, must meet the requirements of GDPA. By January 1, 2027, each governmental entity must identify and document any noncompliant personal data processing activities and create strategies to bring those activities into compliance.[15]

GDPA also establishes generally applicable duties for all Utah governmental entities that include—

- Allowing an individual to request that a governmental entity correct or amend their personal data[16]
- Providing a privacy notice to individuals prior to collection of personal data[17]
- Limiting the use of personal data to what is provided in the notice[18]
- Disposing of personal data according to approved record series retention schedules[19]
- Notifying individuals if their personal data is impacted by a data breach[20]
- To assist governmental entities in implementing these and other data privacy practices, GDPA established the Office of Data Privacy (ODP).[21] Additionally, GDPA established the role of Chief Privacy Officer, appointed by the Governor and confirmed by the Senate, who is also the director of the Office of Data Privacy.[22]
- GDPA also created the role of the Data Privacy Ombudsperson who receives complaints from individuals who believe their data privacy rights have been violated by a governmental entity or have a concern about a governmental entity's privacy practices.[23] To ensure compliance, GDPA gives the State Auditor and the Attorney General's Office enforcement authority.[24]

## GIIPA

GIIPA was codified in March 2004, and establishes the requirements a governmental entity must adhere to when collecting

personally identifiable information (PII) through a government-operated website. According to GIIPA, a governmental entity must include a disclosure that details what data is collected, how it is used, and the measures in place to protect it.[25] As stated in statute, "A governmental entity may not collect personally identifiable information related to a user of the governmental entity's government website unless the entity has taken reasonable steps to ensure that on the day on which the personally identifiable information is collected the governmental entity's website complies with [GIIPA]."[26]


### Record Classification

GRAMA mandates that all records must be classified. Non-public records are classified as either private, controlled, protected, or exempt. All government records are assumed to be public unless specified in GRAMA or elsewhere in a different statute.[27] In Utah, a record series serves as the fundamental organizational structure for managing records statewide, ensuring consistency in classification and access. Without record series, there is no generally applicable standardized system for governing data.

**Private** records may only be released with the consent of the subject of such record or by court order. A record is considered private when it contains PII or sensitive information including but not limited to medical and financial information, welfare benefits, elements of a person's voter registration, or child custody information. Certain government-created records such as legislative ethics reports, independent executive branch ethics reports, employment records of former members of the Department of Justice, and hearings regarding the character, professional competence, or mental health of an individual are also classified as private. There are forty-two types of private records defined in GRAMA.[28-29]

Records classified as **controlled** under GRAMA may only be released under limited circumstances. Controlled records are records containing an individual's medical history which a governmental entity believes would be detrimental to the mental health or safety of an individual if released. It also has the shortest classification requirements section. There is only one type of record that can qualify as a controlled record as defined in GRAMA.[30]

A record is considered **protected** if it contains trade secrets, confidential commercial information, test answers used in academic and employment examinations, or if the release of the record would impair government functions or endanger the safety of an individual. Protected records make up the largest classification portion of the code and also include records such as certain police reports and sensitive information regarding agriculture and critical infrastructure. There are eighty-eight types of records that can fall into this classification.[31]

Any record that is limited by court rule, another state statute, federal statute, or federal regulation is considered **exempt from disclosure.**[32] These records are still subject to the requirements of GRAMA, however, they are not subject to disclosure and access requirements provided in GRAMA, except in limited circumstances.[33] In addition, there may also be other records that are exempted in Utah code that are not included in this list.

**WHAT IS AN EXEMPTION?**

An exemption lets certain people, businesses, or information be left out from a law; a way to make exceptions to a rule.


## The Privacy Program Framework as a Governance Reference

The Utah Office of Data Privacy (ODP) was established by GDPA to "assist state agencies to implement effective and efficient privacy practices, tools, and systems."[34] To fulfill this mandate and the requirements of Executive Order 2023-06,[35] which required Utah's Chief Privacy Officer to create a strategic privacy program plan, ODP released the first version of the Privacy Program Framework on December 17, 2024. This framework is designed "as a resource to assist agencies in meeting [GDPA's] May 1, 2025, deadline."[36] It outlines recommended steps a governmental entity may take to implement a privacy program, defined by the framework as "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."[37] The

| 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 |
| | 6 | Record Series Privacy Annotation |
| Awarenes and Training | 7 | Records Officers Training and Certification |
| | 8 | Statewide Privacy Awareness Training |
| Identify | 9 | Inventorying |
| | 10 | Privacy Impact Assessment |
| Transparency | 11 | Website Privacy Policy |
| | 12 | Privacy Notice (Notice to Provider of Information) |
| Processing | 13 | Minimum Data Necessary |
| | 14 | Record and Data Sharing or Selling |
| | 15 | Record Retention and Disposition |
| Information Security | 16 | Incident Response |
| | 17 | Breach Notification |
| Individual Requests | 18 | Data Subject Requests for Access |
| | 19 | Data Subject Requests for Amdendment or Corrections |
| | 20 | Data Subject Requests for an Explanation |
| | 21 | Data Subject Requests At-Risk Employee Restrictions |

## Privacy Program Framework's 21 Privacy Practices

framework includes two key sections, "Privacy Practices," and the "Privacy Maturity Model."

### Privacy Practices

The Privacy Practices section of the framework details twenty-one generally applicable practices that a governmental entity should implement as part of their program to meet the data governance requirements established in Utah's four foundational data governance laws. These twenty-one practices are divided into eight sections, each section focused on a different category of data governance. After initiating a privacy program that includes the twenty-one outlined practices, a governmental entity can then measure the maturity of their practices using the Privacy Maturity Model.[38]

### Privacy Maturity Model

The Privacy Maturity Model is used to measure and indicate the level of maturity of specific practices within a privacy program. The Privacy Maturity Model expands on the twenty-one privacy practices by offering a structured framework for governmental entities to assess and improve their privacy programs over time. The model progresses from level 0 (non-existent), where no formal privacy practices are in place, to level 5 (optimized), where privacy is fully embedded in agency operations. This maturity model measures compliance and emphasizes continuous improvement, operational effectiveness, and the strategic management of privacy risks, thereby helping governmental entities to evolve—or mature—beyond basic legal adherence toward proactive and resilient privacy programs.[39] It is important to note that increasing maturity of practices requires implementation and completion of strategies and tasks.


# Gaps and Conflicts in Data Governance

Some smaller counties and municipalities may have trouble implementing privacy programs because of their lack of resources. A representative from the League of Cities and Towns stated, "Rural areas are much less equipped with staff and may struggle . . . In some of these municipalities, the mayor is also the public works driver when it snows, the recorder, and the treasurer. They are literally everything because the population is so small."[40] According to Utah County Commissioner Amelia Powers Gardner, "Local governments, particularly smaller counties, cities, or special service districts oftentimes don't have the resources that we really do need to protect people's privacy."[41] According to Utah's Chief Privacy Officer, "The Office of Data Privacy is actively working with governmental entities like Utah Association of Counties and Utah League of Cities and Towns to create standardized and more simplistic tools and resources to accommodate these operational challenges."[42]

## Gaps and Conflicts

- Lack of CAO designation
- Conflicting privacy statements
- Retention schedule non compliance
- Failure to provide a purpose and use statement

### Chief Administrative Officers

DARSMGR requires every governmental entity to have a Chief Administrative Officer (CAO) that is responsible for maintaining a continuous and active records management program that adequately protects individuals' rights, including the right to privacy and transparency, while also ensuring the program facilitates the efficient use of data. The CAO is also responsible for appointing records officers, and responding to appeals when a GRAMA request is denied.[43]

According to the most recent data available from DARS, out of over 2,500 governmental entities in the State of Utah, there are at least around 700 that do not have a designated CAO.[44] DARSMGR does not explicitly state that a governmental entity must designate a CAO, however, it establishes the role and defines duties. Without a CAO, governmental entities are unable to appoint records officers, as required in statute.[45] As one government employee noted, "Nowhere does the code actually state that a governmental entity has to appoint a CAO, it just says 'here are the duties of one.' If someone has duties, there should be somebody who's doing the job functions outlined. But to not even acknowledge that a governmental entity has to appoint one seems like a huge gap in the statute."[46] The absence of a designated CAO

may lead to challenges in ensuring effective data governance, including handling of GRAMA requests or appeals, maintaining compliance with retention schedules, and complying with applicable privacy and transparency laws.[47]

### Data Management Requirements

As previously indicated, GIIPA requires governmental entities to include a privacy notice whenever personal information is gathered through a government-operated website.[48] GRAMA and GDPA also mandate that a governmental entity provide a disclosure when PII is collected.[49-50] It is worth noting that the three privacy notices contain different requirements, and the current code does not specify which notice entities should prioritize, or whether multiple notices should be used in combination. This conflict and lack of clarity may present challenges for governmental entities in determining the most effective way to comply with notice requirements.

Each record series is required to adhere to a retention schedule. A retention schedule stipulates how long the content in a given record series should be retained and how it must be disposed of when the disposition date has been reached.[51] Most records are required to be destroyed at the end of their retention schedule, while certain records with historical or longitudinal value—such as birth certificates—are archived.[52] During a series of interviews, many governmental entities stated they are facing challenges in adhering to record disposal requirements outlined in their retention schedules. When asked if governmental entities are in compliance with their retention schedules, one government employee responded, "I am not aware of any governmental entity that is properly disposing of their collected data."[53] A representative from DARS said, "If every governmental entity adhered to their retention schedule right now, we would not have enough space to accommodate the archived records."[54]

GRAMA mandates that when a governmental entity creates a new records series, it must file a purpose and use statement with the State Archivist, who is also the director of DARS, detailing the intended purpose and use of the record series.[55] These statements are critical to ensuring entities do not misuse data. According to a representative from DARS, "[Many] governmental entities have not submitted purpose and use statements."[56] Without purpose and use statements, there are no documented parameters to determine how data may be used.

## The Benefits of Modernized Data Governance

### Balancing of Interests

A foundational principle of effective data governance is the careful balance between transparency, privacy, and the operational needs of governmental entities. GRAMA establishes this equilibrium by ensuring public access to government records while recognizing legitimate interests in confidentiality and responsible records management.[57]

The Utah Legislature has emphasized that transparency should be the default, allowing the public to access government records in an easy and reasonable manner.[58] However, it also acknowledges that there are instances where restricting access serves the greater public interest, such as protecting privacy, ensuring security, and maintaining the integrity of governmental operations.[59] GRAMA prevents arbitrary confidentiality by allowing restrictions only when explicitly justified, aligning with national standards for information governance.

A well-functioning data governance framework must go beyond simply granting or restricting access—it must also ensure that disclosed information is useful, structured, and contextually meaningful.[60] When both transparency and privacy are prioritized over the practical usability of data, information may become available in a fragmented, overly restricted, or difficult-to-interpret form.[61] This can create a paradox where data is technically accessible but functionally unusable thereby limiting public engagement, accountability, and innovation. Transparency efforts must therefore balance openness with stewardship and usefulness. Without proper structuring, interoperability, and contextualization, public records may fail to serve their intended purpose.[62]

Conversely, when governments and organizations focus too heavily on data-driven decision-making without sufficient oversight, ethical and regulatory risks emerge.[63] The unchecked collection, use, and linkage of data can lead to unintended harms, including privacy violations and the erosion of public trust. Strong records management policies help mitigate these risks by ensuring that data is used responsibly, with clear guidelines for collection, retention, and access.[64]

### Considerations for Efficiency

Commissioner Amelia Powers Gardner recently stated, "In an ever more digital world, it is more and more difficult for us to come into compliance with these statutes."[65] The proliferation of digital tools and systems has transformed how data is collected, stored, shared, and protected, necessitating an evolution in both legal frameworks and governance practices. Addressing gaps in

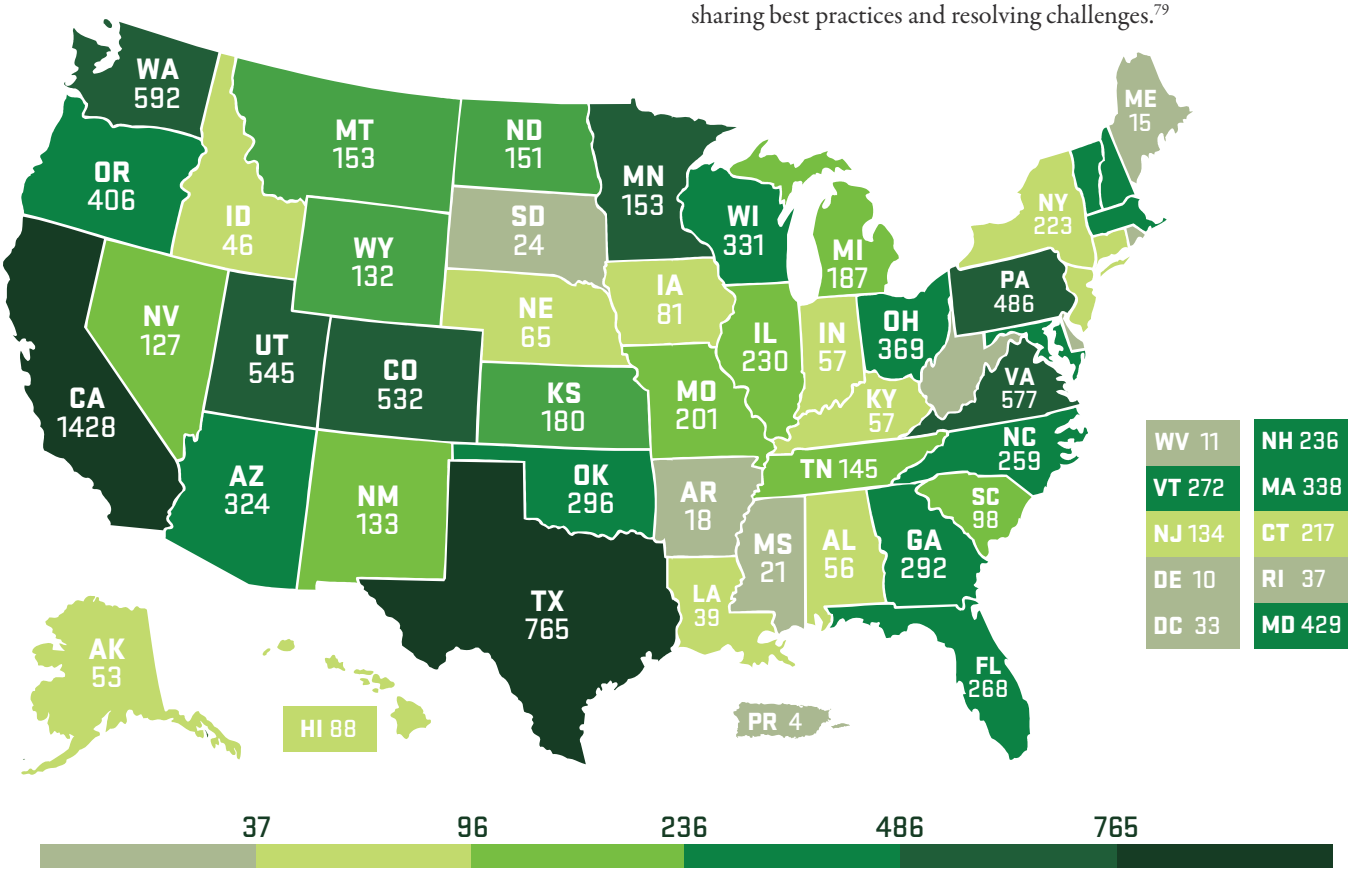
existing statutes and modernizing data governance policies would not only enhance government efficiency and transparency but also strengthen privacy protections.[66]

Modernized data governance could enhance efficiency and consistency across governmental entities.[67] Standardized protocols for data sharing, security, and records management would streamline operations, reduce redundancies, and ensure a more cohesive approach to data stewardship. By adopting uniform policies, governmental entities can improve privacy safeguards, bolster public trust, and demonstrate compliance with evolving legal and regulatory requirements.[68] Accountability and compliance will lead to a more transparent environment, and are central to an effective data governance model.[69] Constituents will benefit from stronger privacy protections as governmental entities adopt standardized measures for securing personal information.[70] By adhering to modernized data governance policies and practices, governmental entities can simultaneously promote transparency and mitigate risks to individuals.[71]

Modernized data governance could also improve data security and help to standardize risk management. Standardized risk assessments and incident response protocols could enable faster and more coordinated responses to potential data breaches.[72] Enhanced and standardized data governance practices could also support data-driven decision-making, thereby allowing for further data analysis.[73] Innovation will be enhanced with access to better, more relevant data.[74] With more reliable data, governmental entities could harness predictive analytics to allocate resources more effectively, address community needs proactively, and innovate in areas such as public health and urban planning.[75] Utah has the opportunity to set a national example for how governmental entities can use data to foster transparency, improve services, and empower communities in the digital age. Utah is already actively engaging in critical discussions surrounding data governance and emerging as a thought leader in the field.[76]

## Considerations for Modernizing Data Governance

As governmental entities work to improve their data governance practices, cross-entity collaboration on data management strategies may help them become compliant, share ideas, eliminate confusion, and promote consistent protections across the state.[77] Collaboration may also cultivate shared responsibility, allowing entities to learn from each other, reduce redundancy, and support a cohesive statewide approach.[78] Governmental entities could also establish working groups, advisory panels, or online platforms for sharing best practices and resolving challenges.[79]




**Occurrences of the Term "Data Governance" in Public Government Proceedings**

Considering the importance of collaboration and shared responsibility in the governance process, ensuring privacy and transparency could be a cornerstone of these efforts. Drawing from anonymous interviews, current legal code, and outside sources, the following policy modernizations could be considered:

- Codify the requirement to designate a CAO
- Include "privacy and transparency" in CAO responsibilities
- Implement a CAO annual reporting model to track progress and identify persistent issues in privacy, transparency, and records management efforts
- Require CAOs to report to DARS who they have designated as records officers annually
- Expand Privacy Program Framework to include all generally applicable practices related to transparency and records management
- Enact stricter enforcement mechanisms for noncompliance regarding retention schedules and purpose and use statements
- Consider consolidation of the three collection statements from GRAMA,[80] GDPA,[81] and GIIPA[82]

Considering the importance of collaboration and shared responsibility in the governance process, ensuring privacy and transparency could be a conerstone of these efforts. Drawing from anonymous interviews, current legal code, and outside sources, the following policy modernizations could be considered:

- Codify the requirement to designate a CAO
- Include "privacy and transparency" in CAO responsibilities

Implement CAO annual reporting model to track progress and identify persistent issues in privacy, transparency, and records management efforts

- Require CAOs to report to DARS who they have designated as records officers annually
- Expand the Privacy Program Framework to include all generally applicable practices related to transparency and records management
- Enact stricter enforcement mechanisms for noncompliance regarding retention schedules and purpose and use statements
- Consider consolidation of the three collection statements from GRAMA,[80] GDPA,[81] and GIIPA[82]

### Using the Privacy Program Framework to Build a Statewide Data Governance Model

The Privacy Program Framework serves as a robust foundation for governmental entities seeking to implement structured and accountable data governance. While originally designed to establish privacy best practices, the framework also aligns with broader records management and transparency requirements—critical components of a modern data governance strategy. Although it does not encompass all sector-specific data regulations, such as HIPAA and FERPA, or fully address every transparency and records management obligation, the framework offers a universal starting point that ensures consistency across all governmental entities in Utah.

Recognizing its potential as a statewide data governance foundation, the Utah Valley University Herbert Institute has reviewed and endorsed this framework as the basis for developing a comprehensive, unified data governance model. The structured, principle-based approach embedded in the framework allows entities to customize governance practices to their operational needs while maintaining a consistent, interoperable structure at the state level. Research on governance frameworks underscores that an integrated privacy and data governance strategy strengthens compliance, enhances public trust, and improves data stewardship.[83]

A key advantage of this framework is its ability to establish a common thread of data governance definitions and measures across all governmental entities, uniquely positioning Utah to expand and refine its data governance model. The first five privacy practices outlined in the framework—designating a CAO, appointing records officers, creating record series, classifying records and establishing data retention schedules—are broadly applicable to all government entities. These foundational elements ensure that privacy, transparency, and data governance operate in concert rather than as competing obligations. While the framework does not directly modify Utah's legal code, it proactively addresses many gaps in existing statutes by defining and standardizing privacy and data governance responsibilities in an operational data lifecycle view.

By adopting the privacy practices outlined in the framework, governmental entities can progress through the Privacy Maturity Model, strengthening compliance with data governance laws while enhancing accountability and public trust.[84] By leveraging the Privacy Program Framework as the cornerstone of a statewide data governance model, Utah can build an adaptable, scalable governance structure that evolves with technological advancements and regulatory needs. The continued expansion of resources— such as maturity models, implementation tools, and best practice guides—will further empower governmental entities to navigate an increasingly complex data landscape with confidence and accountability.[85]

### GovSense: An AI Model Supporting Effective Data Governance

UVU's Smith College of Engineering and Technology has partnered with the ODP to create an AI model called GovSense to evaluate and assist agencies in modernizing data governance.

GovSense is an AI-driven solution that helps government agencies meet legal obligations for records management, privacy protection, and regulatory compliance. It consolidates critical documents, streamlines audits, and minimizes legal risks. By ensuring consistent data policies and automated compliance checks, GovSense supports transparency while reducing manual paperwork.

GovSense will use Utah code to create a knowledge base of all statutory requirements for data governance. This model aims to help government agencies meet regulatory compliance for records management and comply with privacy protection. It will streamline audits and minimize legal risks.

GovSense focuses on privacy and accuracy. It offers quick access to statutes and procedural guidelines, freeing legal teams to concentrate on providing counsel and protecting public interests. With GovSense, agencies can stay compliant and improve efficiency without sacrificing security or thoroughness.

## Conclusion and Next Steps

The current data governance framework found in GRAMA, GDPA, DARSMGR, and GIIPA provides a foundation for protecting personal data. However, ambiguous sections of Utah's code and the lack of consistent implementation across state and municipal agencies highlight the need for modernization.

The Herbert Institute for Public Policy has evaluated the Privacy Program Framework and determined it will likely enable entities to align with privacy standards through structured practices. By adopting the recommendations within the Privacy Practices section, governmental entities can advance through the Privacy Maturity Model, thus enhancing compliance with data governance laws. This progressive approach ensures legal adherence and builds public trust, demonstrating a commitment to upholding privacy rights securely and efficiently.

Furthermore, modernization of the state code can address ambiguities that may hinder progress and enforcement. With plans to update the code during the 2025 legislative session by creating a clear, comprehensive legal framework, Utah will become a national example in data governance. The continued development of resources like the Privacy Program Framework will provide valuable guidance and tools for entities to navigate the challenges of data governance.

# Bibliography


1. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2.html?v=C63G-2_1800010118000101

2. Utah State Legislature. Division of Archives and Records Service and Management of Government Records. Utah Code § 63A-12-1. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63A/Chapter12/63A-12-P1.html?v=-C63A-12-P1_2021050520210505

3. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19.html

4. Utah State Legislature. Government Internet Information Privacy Act. Utah Code § 63D. Accessed December 29, 2024. https://le.utah.gov/xcode/Title63D/63D.html

5. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-102. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S102.html

6. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-102. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S102.html

7. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-103. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S103.html?v=C63G-2-S103_2024050120240501

8. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-307. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S307.html?v=C63G-2-S307_2023050320230503

9. Utah State Legislature. Division of Archives and Records Service and Management of Government Records. Utah Code § 63A-12-101. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter12/63A-12-S101.html?v=-C63A-12-S101_2023050320230503

10. Kichas, Jim. Our History: The Early Years. Utah Division of Archives and Records Service, October 9, 2019. Accessed December 20, 2024. https://archives.utah.gov/2019/10/09/our-history-the-early-years/

11. Utah State Legislature. Division of Archives and Records Service and Management of Government Records. Utah Code § 63A-12. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63A/Chapter12/63A-12.html

12.Utah State Legislature. Division of Archives and Records Service and Management of Government Records. Utah Code § 63A-12-101. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter12/63A-12-S101.html?v=-C63A-12-S101_2023050320230503

13. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-401. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=-C63A-19-S401_2024050120240501

14. Interview with a government employee, December 10, 2024.

15. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-401. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=-C63A-19-S401_2024050120240501

16. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-403. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S403.html?v=-C63A-19-S403_2024050120240501

17. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-402. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S402.html

18. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-402. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S402.html

19. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-404. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S404.html

20. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-406. Accessed February 9, 2025. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S406.html

21. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-9-301. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S301.html?v=-C63A-19-S301_2024050120240501

22. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-302. Accessed February 9, 2025. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S302.html?v=-C63A-19-S302_2024050120240501

23. Utah State Legislature. Government Data Privacy Act. Utah

Code § 63A-19-501. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S501.html?v=C63A-19-S501_2024050120240501

24. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-601. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S601.html?v=C63A-19-S601_2024050120240501

25. Utah State Legislature. Government Internet Information Privacy Act. Utah Code § 63D-2-103. Accessed December 29, 2024. https://le.utah.gov/xcode/Title63D/Chapter2/63D-2-S103.html?v=C63D-2-S103_1800010118000101

26. Utah State Legislature. Governmental Internet Information Privacy Act. Utah Code § 63D-2-103 (1). February 9, 2025. https://le.utah.gov/xcode/Title63D/Chapter2/63D-2-S103.html

27. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-201. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S201.html?v=C63G-2-S201_2023050320230503

28. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-302. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S302.html?v=C63G-2-S302_2024070120240501

29. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-303. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S303.html

30. Utah State Legislature. Government Records Access and Management Act. Code § 63G-2-304. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S304.html

31. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-305. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S305.html

32. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-201 (3) (b). Accessed February 9, 2025. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S201.html

33. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-201. Accessed December 17, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S201.html?v=C63G-2-S201_2023050320230503

34. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-301. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S301.html?v=C63A-19-S301_2024050120240501

35. Governor Spencer J. Cox. Executive Order 2023-06, Directing the Chief Privacy Officer to Develop a Strategic Privacy Plan. August 1, 2023. Accessed January 31, 2025. https://drive.google.com/file/d/16R4kLIatmNhXnd67MrqtTnEJzHXf8I6G/view

36. Utah Office of Data Privacy. Privacy Program Framework. Page 2. December 17, 2024. Accessed December 19, 2024. https://privacy.utah.gov/wp-content/uploads/Office-of-Data-Privacy-Privacy-Program-Framework_v1_2024.12.11_final.pdf

37. Utah Office of Data Privacy. Privacy Program Framework. Page 2. December 17, 2024. Accessed December 19, 2024. https://privacy.utah.gov/wp-content/uploads/Office-of-Data-Privacy-Privacy-Program-Framework_v1_2024.12.11_final.pdf

38. Utah Office of Data Privacy. Privacy Program Framework. Page 7. December 17, 2024. Accessed December 19, 2024. https://privacy.utah.gov/wp-content/uploads/Office-of-Data-Privacy-Privacy-Program-Framework_v1_2024.12.11_final.pdf

39. Utah Office of Data Privacy. Privacy Program Framework. Page 22. December 17, 2024. Accessed December 19, 2024. https://privacy.utah.gov/wp-content/uploads/Office-of-Data-Privacy-Privacy-Program-Framework_v1_2024.12.11_final.pdf

40. Interview with a representative from the League of Cities and Towns, December 19, 2024.

41. Gardner, Amelia Powers. House Government Operations Committee. Filmed February 20, 2024. Utah State Legislature, 2:05:44. Accessed January 7, 2025. https://le.utah.gov/av/committeeArchive.jsp?timelineID=250765

42. Interview with Chief Privacy Officer, January 31, 2025.

43. Utah State Legislature. Division of Archives and Records Service and Management of Government Records. Utah Code § 63A-12-103. Accessed December 19, 2024. https://le.utah.gov/xcode/Title63A/Chapter12/63A-12-S103.html?v=C63A-12-S103_2021050520210701

44. DARS Data, "Entities Without a CAO", 1/31/25, in author's possession

45. Utah State Legislature. Division of Archives and Records

Service and Management of Government Records. Utah Code § 63A-12-103. Accessed December 19, 2024. https://le.utah.gov/xcode/Title63A/Chapter12/63A-12-S103.html?v=C63A-12-S103_2021050520210701

46. Interview with a government employee, December 18, 2024.

47. Relly, Jeannine E., and Meghna Sabharwal. Perceptions of Transparency of Government Policymaking: A Cross-National Study. Government Information Quarterly 26, no. 1 (January 2009): 148–57. https://doi.org/10.1016/j.giq.2008.04.002.

48. Utah State Legislature. Government Internet Information Privacy Act. Utah Code § 63D-2-103. Accessed December 29, 2024. https://le.utah.gov/xcode/Title63D/Chapter2/63D-2-S103.html?v=C63D-2-S103_1800010118000101

49. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-601. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S601.html?v=C63G-2-S601_2023050320230503#63G-2-601(2)

50. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-402. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S402.html

51. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-604. Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S604.html?v=C63G-2-S604_2023050320230503

52. Utah State Legislature. Division of Archives and Records Service and Management of Government Records. Utah Code § 63A-12-101. Accessed December 19, 2024. https://le.utah.gov/xcode/Title63a/Chapter12/63a-12-S101.html

53. Interview with government official, December 10, 2024.

54. Interview with government official, December 19, 2024.

55. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-601 (4). Accessed December 16, 2024. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S601.html?v=C63G-2-S601_2023050320230503

56. Interview with government official, December 19, 2024.

57. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-102 (1). Accessed February 7, 2025. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S102.html

58. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-102 (3). Accessed February 7, 2025. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S102.html

59. 35. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-102. Accessed December 18, 2024. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S102.html

60. Young, Meg, Luke Rodriguez, Emily Keller, Feiyang Sun, Boyang Sa, Jan Whittington, and Bill Howe. "Beyond Open vs. Closed." Proceedings of the Conference on Fairness, Accountability, and Transparency, January 29, 2019, 191–200. https://doi.org/10.1145/3287560.3287577.

61. Janssen, Marijn, and Jeroen van den Hoven. "Big and Open Linked Data (BOLD) in Government: A Challenge to Transparency and Privacy?" Government Information Quarterly 32, no. 4 (October 2015): 363–68. https://doi.org/10.1016/j.giq.2015.11.007.

62. Borgesius, Frederik Zuiderveen, Jonathan Gray, and Mireille van Eechoud. "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework." Berkeley Law, May 2015. https://lawcat.berkeley.edu/record/1127406?v=pdf.

63. Wu, Chao. "Data Privacy: From Transparency to Fairness." Technology in Society 76 (March 2024). https://doi.org/10.1016/j.techsoc.2024.102457.

64. Olateju, Omobolaji, Samuel Ufom Okon, Oluwaseun Oladeji Olaniyi, Amaka Debie Samuel-Okon, and Christopher Uzoma Asonze. "Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data." SSRN Electronic Journal, June 27, 2024. https://doi.org/10.2139/ssrn.4879025.

65. Gardner, Amelia Powers. House Government Operations Committee. Filmed February 20, 2024. Utah State Legislature, 2:05:44. Accessed January 7, 2025. https://le.utah.gov/av/committeeArchive.jsp?timelineID=250765

66. Digital Regulation Platform. Navigating Data Governance: A Guiding Tool for Regulators. Digital Regulation Platform, October 31, 2024. Accessed January 9, 2025. https://digitalregulation.org/navigating-data-governance-a-guiding-tool-for-regulators/

67. Khatri, Vijay, and Carol V. Brown. Designing Data Governance. Communications of the ACM 53, no. 1 (January 2010): 148–52. https://doi.org/10.1145/1629175.1629210.

68. Seavers, Michael L. Citizen's perception and use of governmental transparency: Effects on citizen trust and participation in government. Ann Arbor: ProQuest Dissertations & Theses, 2018.

69. Jimenez Jaramillo, Aleja. A comparative analysis of Domestic Municipal Data Governance Systems. Cambridge, MA: Massachusetts Institute of Technology, 2023.

70. Engelenburg, Sélinde van, Marijn Janssen, and Bram Klievink. Design of a Software Architecture Supporting Business-to-Government Information Sharing to Improve Public Safety and Security. Journal of Intelligent Information Systems 52, no. 3 (July 27, 2017): 595–618. https://doi.org/10.1007/s10844-017-0478-z.

71. Paunov, Yavor, Michaela Wänke, and Tobias Vogel. Transparency Effects on Policy Compliance: Disclosing How Defaults Work Can Enhance Their Effectiveness. Behavioral Public Policy 3, no. 02 (November 9, 2018): 187–208. https://doi.org/10.1017/bpp.2018.40.

72. Price, Joseph Derek. Reducing the risk of a data breach using effective compliance programs. Minneapolis, Minnesota: Walden University, 2014.

73. Ishmail, Zeenat. Data governance in the public sector: A data governance model for the strategic use of data at the sub-national level. Johannesburg: University of Johannesburg, South Africa, 2024.

74. Bartolomucci, Federico, and Francesco Leoni. Designing an Effective Governance Model for Data Collaboratives. Research-Technology Management 67, no. 4 (June 27, 2024): 49–61. https://doi.org/10.1080/08956308.2024.2351331.

75. Ho, Duy H., and Yugyung Lee. Big Data Analytics Framework for Predictive Analytics Using Public Data with Privacy Preserving. 2021 IEEE International Conference on Big Data (Big Data), December 15, 2021, 5395–5405. https://doi.org/10.1109/bigdata52589.2021.9671997.

76. Allen, Paul. Data Governance Heat Map. CitizenPortal.ai - Search Summary. Accessed January 29, 2025. https://citizenportal.ai/summary?qq=data+governance&lastDays=0.

77. Chukwurah, Naomi, Adebimpe Bolatito Ige, Victor Ibukun Adebayo, and Osemeike Gloria Eyieyien. Frameworks for Effective Data Governance: Best Practices, Challenges, and Implementation Strategies across Industries. Computer Science & IT Research Journal 5, no. 7 (July 25, 2024): 1666–79. https://doi.org/10.51594/csitrj.v5i7.1351.

78. Chen, Yu-Che, and Jooho Lee. Collaborative Data Networks for Public Service: Governance, Management, and Performance. Public Management Review 20, no. 5 (March 31, 2017): 672–90. https://doi.org/10.1080/14719037.2017.1305691.

79. Paprica, P Alison, Monique Crichlow, Donna Curtis Maillet, Sarah Kesselring, Conrad Pow, Thomas P. Scarnecchia, Michael J. Schull, et al. Essential Requirements for the Governance and Management of Data Trusts, Data Repositories, and Other Data Collaborations. International Journal of Population Data Science 8, no. 4 (September 20, 2023). https://doi.org/10.23889/ijpds.v8i4.2142.

80. Utah State Legislature. Government Records Access and Management Act. Utah Code § 63G-2-601. Accessed January 29, 2025. https://le.utah.gov/xcode/Title63G/Chapter2/63G-2-S601.html

81. Utah State Legislature. Government Data Privacy Act. Utah Code § 63A-19-402. Accessed January 29, 2025. https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S402.html

82. Utah State Legislature. Government Internet Information Privacy Act. Utah Code § 63D-2-103. January 29, 2025. https://le.utah.gov/xcode/Title63D/Chapter2/63D-2-S103.html?v=C63D-2-S103_1800010118000101

83. Chukwurah, Naomi, Adebimpe Bolatito Ige, Victor Ibukun Adebayo, and Osemeike Gloria Eyieyien. Frameworks for Effective Data Governance: Best Practices, Challenges, and Implementation Strategies across Industries. Computer Science & IT Research Journal 5, no. 7 (July 25, 2024): 1666–79. https://doi.org/10.51594/csitrj.v5i7.1351.

84. Utah Office of Data Privacy. Privacy Program Framework. Page 21. December 17, 2024. Accessed January 29, 2025. https://privacy.utah.gov/wp-content/uploads/Office-of-Data-Privacy-Privacy-Program-Framework_v1_2024.12.11_final.pdf

85. Borgesius, Frederik Zuiderveen, Jonathan Gray, and Mireille van Eechoud. "Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework." Berkeley Law, May 2015. https://lawcat.berkeley.edu/record/1127406?v=pdf.

**Gary R. Herbert Institute Staff and Advisors**

LEADERSHIP TEAM
Gary R. Herbert, Founder, 17th Governor, Utah
Justin Jones, MS, Executive Director
Dan Dimond, Sr. Director Institutional Advancement, UVU Foundation
Liv Moffat, Development Director, Herbert Foundation
Erik Nystul, Program Director, Government Internships
Karen Gill, Events
Becca Aylworth Wright, Communications

FACULTY FELLOWS
Tara Bishop, PhD, Assist. Prof. Earth Science / Enviro Mgmt, Earth Sciences, Herbert Fellow
Lauren Brooks, PhD, Assistant Professor of Biology, Herbert Fellow
John Kidd, PhD, Assist. Prof. Statistics, Herbert Fellow
Alan Parry, PhD, Assoc. Prof. Mathematics, Herbert Fellow

RESEARCH INTERNS
Cade Bloomer, Research Intern
Katelyn Carpenter, Events and Social Media Intern
Sophia Clark, Events Intern
William Freedman, AI/Deepfake Research Intern
Tyler Gurney, AI/Deepfake Research Intern
Jessica Hollingsworth, Graphic Design Intern
Josh Jorgensen, Judicial Trust, Research Intern
Jonathan (Jon) Kwong, Communications Intern
Canyon Moser, WRI, Research Intern
Addison Stott, WRI, Elections Trust, Research Intern
John Nelson, Graphic Design Intern