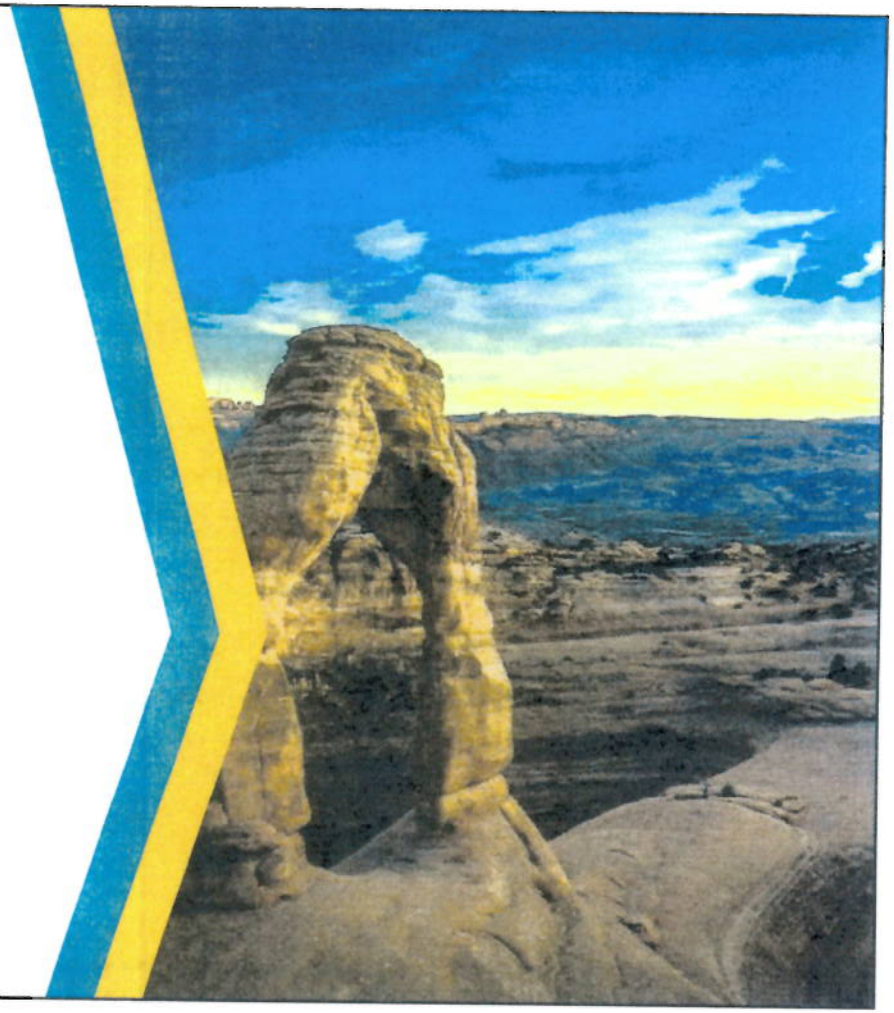
Government Data Privacy Act

HB 491

Rep. Jefferson Moss



HB 491 Summary

HB 491 creates a foundation on which future incremental efforts and legislation will be built while immediately putting into law new key privacy protections for the public, new privacy governance structure for governmental entities, enhancements to existing governance structure to improve outcomes, basic enforcement, and remedy mechanisms to enable the public to hold governmental entities accountable for meeting their privacy obligations.

Drivers:
OLAG Recommendations

UTAH STATE LEGISLATURE
Office of the Legislative Auditor General

OLAG Report No. 2023-07

OLAG Recommendation 1.1

The Legislature should consider if guardrails are needed to balance the benefits of data and data sharing with data privacy practices in agencies.

OLAG Recommendation 1.2

The Legislature should consider the merits of passing a data privacy act into statute to provide a data privacy governance structure for state agencies and incorporate data privacy principles into their data processing and sharing practice.

Drivers:
OLAG Recommendations

PAST DATA PRACTICES

- Paper files
- Laborious manual entry
- Limited data collection and sharing

CURRENT DATA PRACTICES

- Evolution of technology
- Mass data collection and sharing
- Upgraded data systems
- No overarching statute to control data flow

POTENTIAL FUTURE DATA PRACTICES

- Statute to provide guardrails for agencies
- Secure data
- Controlled data collection

Drivers:
Reports, Executive Orders and Assessments

CPO

2022 JIC Report

Executive Order 2023-06

UTAH STATE LEGISLATURE
Office of the Legislative Auditor General

Report No. 2023-07

CPO

2023 Assessments and JIC Report

PPOC

PPOC Privacy Practice Reviews

Drivers:
Current Utah Laws Impacting Privacy

Utah's current privacy laws are best described as disparate, fragmented, not comprehensive, conflicting and as having gaps. These include:

Division of Archives and Records Services
Utah Code § 63A-12-100 *et seq.*
Government Records Access and Management Act
Utah Code § 63G-2-101 *et seq.*
Governmental Internet Information Privacy Act
Utah Code § 63D-2-101 *et seq.*
Chief Privacy Officer
Utah Code § 67-1-17
Personal Privacy Oversight Commission
Utah Code § 63C-24-101 *et seq.*
State Privacy Officer (Auditor)
Utah Code § 67-3-13
Unauthorized Access to Information Technology
Utah Code § 63D-3-101 *et seq.*
Utah Technology Governance Act. Chief Information Officer.
Utah Code § 63A-16-210
Single Sign-on Portal
Utah Code § 63A-16-801 *et seq.*

Utah Open Records Portal Website
Utah Code § 63A-12-114
Utah Open Data Portal Website
Utah Code § 63A-16-107
Utah Public Notice Website
Utah Code § 63A-16-601 through 602
Utah Transparency Advisory Board
Utah Code § 63A-18-101 *et seq.*
Cybersecurity Affirmative Defense Act
Utah Code § 78B-4-701 *et seq.*
Uniform Electronic Transactions Act
Utah Code § 46-4-101 *et seq.*
Electronic Records in Government Agencies
Utah Code § 46-4-501--503
R895-8.
State Privacy Policy and Agency Privacy Policies
State Issued Identification Number Act
Utah Code § 63G-15-101 *et seq.*

Drivers:
Federal Laws Impacting Privacy Include:

The Health Insurance Portability and Accountability Act (HIPAA)	The Family Educational Rights and Privacy Act (FERPA)	The Fair Credit Reporting Act (FCRA)
The Gramm-Leach-Bliley Act (GLBA)	The Children's Online Privacy Protection Act (COPPA)	The Electronic Communications Privacy Act (ECPA)
The Telephone Consumer Protection Act (TCPA)	The Video Privacy Protection Act (VPPA)	The Genetic Information Nondiscrimination Act (GINA)

Legislation Workgroup and Stakeholder Engagement

- 25+ workgroup and stakeholder engagement meetings
- Three presentations to Personal Privacy Oversight Commission
- Two Presentations to Judiciary Interim Committee
- One Presentation to UEOC

State Data Privacy Policy
Section 63A-19-102

Creates a state privacy policy (similar to the state energy policy Section 79-6-301), high level concepts that frame how the governing board, commission and Office of Data Privacy will approach recommendations for building privacy for Utah with respect to all governmental entities.

The data privacy policy emphasizes the fundamental interest and expectation of privacy regarding personal data provided to governmental entities.

It outlines the necessity for governmental entities to respect individuals' privacy rights, encourage innovation in data protection measures, and promote employee training on data privacy best practices. Additionally, the policy aims to promote enhancements in future policies, including clear notice, minimal data processing, consent mechanisms, individual data access and control, safeguard implementation, compliance accountability, and consistency in data privacy terminology across governmental entities.

Utah Privacy Governing Board
Section 63A-19-201

The Utah Privacy Governing Board, comprised of five members, including the following or their designees: the Governor, President of the Senate, the Speaker of the House of Representatives, the attorney general, and the state auditor.

The governing board is similar in composition to other boards, commissions, and councils that include representation from different branches of government to address significant issues, such as:

Cybersecurity Commission, Section 63C-27-101

Constitution Defense Council, Section 63C-4a-101

State Capitol Preservation Board, Section 63C-9-101

Behavioral Health Crisis Response Commission, Section 63C-19-101

Utah Privacy Governing Board
Section 63A-19-201

The governing board is tasked with:

- recommending changes to the state data privacy policy;
- approving data privacy agenda items of the Utah privacy commission;
- referring privacy issues raised by the ombudsperson to the State Auditor;
- evaluating the structure and authority of the office of data privacy within state government;
- recommending funding mechanisms for governmental entities to meet data privacy compliance requirements.

Office of Data Privacy
Section 63A-19-301

- Creates the Office of Data Privacy within the Department of Government Operations.
- The office is responsible for creating and maintaining a strategic data privacy plan, reviewing statutory provisions related to governmental data privacy, monitoring high-risk data processing activities, coordinating incident response and reporting plans for data breaches, and providing data privacy training programs for governmental entity employees.
- Provides expertise and assistance to governmental entities for high-risk data processing activities, subject to resource availability.
- Provides support to the Utah Privacy Governing Board.

Duties of Governmental Entities
Section 63A-19-401

HB 491 establishes baseline requirements that apply when no other more specific law applies.

63A-19-401:

If a governmental entity or a contractor described in Subsection (4)(a) is subject to a more restrictive or specific provision of law than found in this part, the governmental entity shall comply with the more restrictive or specific provision of law.

Duties of Governmental Entities
Sections 63A-19-401 through 406

Baseline privacy obligations (some are pre-existing requirements and some are new).

1. Have a privacy program (Partially existing from Section 63A-12-103)
2. Provide Notice of purpose and use of personal data (Existing/GRAMA)
3. Limit use of personal data to what is provided in the notice. (Partially existing/GRAMA)
4. Provide method to request to amend/correct personal data (Existing/GRAMA)
5. Disposition (retention) of personal data (Existing/GRAMA)
6. Do not share personal data unless permitted by law (Existing/GRAMA)
7. Do not sell personal data without express legal requirement (New)
8. Collect and process the minimum amount of personal data necessary. (New)
9. Breach notification to cyber center (Partially new)
10. Breach notification to individuals whose personal data is compromised in a breach. (New)
11. Complete privacy training (New)
12. Maintain inventory and strategy for non-compliant processing activities (New)
13. Report data selling and sharing activities to the CPO or SPO (New)

Duties of Governmental Entities
Sections 63A-19-401

Requirements with future implementation dates/deadlines

(2) A governmental entity:

(a) shall implement and maintain a privacy program before **May 1, 2025**, that includes the governmental entity's policies, practices, and procedures for the process of personal data;

(d) shall meet the requirements of this part for all processing activities implemented by a governmental entity after **May 1, 2024**;

(e) shall for any processing activity implemented before **May 1, 2024**, as soon as is reasonably practicable, but no later than **January 1, 2027**:
(i) identify any non-compliant processing activity:
(ii) document the non-compliant processing activity; and
(iii) prepare a strategy for bringing the non-compliant processing activity into compliance with this part;

Duties of Governmental Entities
Sections 63A-19-401

Impact on Contractors

(4)

(a) A contractor that enters into or renews an agreement with a governmental entity after May 1, 2024, and processes or has access to personal data as a part of the contractor's duties under the agreement, is subject to the requirements of this chapter with regard to the personal data processed or accessed by the contractor to the same extent as required of the governmental entity.

(b) An agreement under Subsection (4)(a) shall require the contractor to comply with the requirements of this chapter to the same extent as the governmental entity.

(c) The requirements under Subsections (4)(a) and (b) are in addition to and do not replace any other requirements or liability that may be imposed for the contractor's violation of other laws protecting privacy rights or government records.

Breach Notice to Cyber Center and AGO
Section 63A-19-405

- A governmental entity that identifies a data breach affecting 500 or more individuals shall notify the Cyber Center and the attorney general of the data breach.
- A governmental entity that experiences a data breach affecting fewer than 500 individuals shall create an internal incident report containing the information in Subsection (2)(b) as soon as practicable.
- An annual report logging all of the governmental entities data breach incidents affecting fewer than 500 individuals shall be provided to the cyber center annually.

Breach Notice to Individuals
Section 63A-19-406

- A governmental entity shall provide a data breach notice to an individual or legal guardian of an individual affected by the data breach.
- The data breach notice to an affected individual shall include:
  - a description of the data breach;
  - the individual's personal data that was accessed or may have been accessed;
  - steps the governmental entity is taking or has taken to mitigate the impact of the data breach;
  - recommendations to the individual on how to protect themselves from identity theft and other financial losses; and
  - any other language required by the Cyber Center.
- Notice shall be provided by email or mail, or other methods as appropriate.

Data Privacy Ombudsperson
Section 63A-19-501

- The governor shall appoint a data privacy ombudsperson with the advice of the governing board.
- The ombudsperson shall serve as a resource for an individual who is making or responding to a complaint about a governmental entity's data privacy practice.
- The ombudsperson may, upon request by a governmental entity or individual, mediate data privacy disputes between individuals and governmental entities.
- The ombudsperson may raise issues and questions before the governing board regarding serious and repeated violations of data privacy from:
  (a) a specific governmental entity; or
  (b) widespread governmental entity data privacy practices.

Remedies/Enforcement
Section 63A-19-601

(1) Upon instruction by the board, the state auditor shall:

a. investigate alleged violations of this chapter by a governmental entity;

b. provide notice to the relevant governmental entity of an alleged violation of this chapter; and

c. for a violation that the state auditor substantiates, provide an opportunity for the governmental entity to cure the violation within 30 days.

(2) If a governmental entity fails to cure a violation as provided in Subsection (1)(c), the state auditor shall report the governmental entity's failure:

a. for a designated government entity, to the attorney general for enforcement under Subsection (3); and

b. for a state agency, to the Legislative Management Committee.

(3) After referral by the state auditor under Subsection (2)(a), the attorney general may file an action in district court to enjoin a violation of or require a governmental entity to comply with this chapter.

Utah Privacy Commission
Section 63C-24-101

- Renames the personal privacy oversight commission as the Utah Privacy Commission.
- Requires the commission to create an annual agenda that identifies:
  - governmental entity privacy practices to be reviewed by the commission;
  - educational and training materials that the commission intends to develop;
  - any other items related to data privacy the commission intends to study; and
  - best practices and guiding principles that the commission plans to develop related to government privacy practices.
- May review and provide recommendations regarding consent mechanisms.
- May provide recommendations to balance transparency, privacy, and data protection.