



UTAH OFFICE *of*
DATA PRIVACY

Legislative Update

VIRTUAL WORKSHOP

*The information in this presentation is provided as a resource to assist governmental entities and **does not constitute legal advice**. Governmental entities should consult with their legal counsel regarding this information.*

Bills Passed



HB 55

Privacy Compliance for Education
Technology Vendors

Rep Auxier/Sen Johnson

Requires contracts between an education entity and a contractor to include privacy requirements.

HB 59

Identification Verification
Amendments

Rep Eliason/Sen Vickers

Requires DABS licensees to verify age only if an individual appears to be younger than 35.

HB 102

Victim Privacy Amendments

Rep Hayes/Sen Pitcher

Requires a victim's initials be used instead their full name on public documents.

HB 199

Health Data Amendments

Rep Thurston/Sen
Cullimore

Revises DHHS's data privacy sharing and security requirements.

HB 220

Public Safety Data Amendments

Rep Wilcox/Sen Cullimore

Makes changes to the information that must be reported to CCJJ and included in the Public Safety Portal.

HB 261

Electronic Information Privacy Act
Amendments

Rep Kyle/Sen Weiler

Clarifies and amends procedures and requirements for law enforcement to process electronic information or records.

HB 319

Electronic Records Amendments

Rep Cutler/Sen Harper

Modifies requirements for the use of digitally authenticated records.

HB 325

Government Records Classification
Amendments

Rep Shepherd/Sen
Stratton

Protects information about victims and those who receive a tax abatement.

Bills Passed



HB 357

Amendments to Motor Vehicle Data Privacy

Rep Chevrier/Sen Harper

Requires motor vehicle manufacturers to comply with the requirements of the Utah Consumer Privacy Act

HB 450

Data Privacy Amendments

Rep Shallenberger/Sen Cullimore

Makes changes to the data privacy requirements for governmental entities.

SB 123

Privacy and Cybersecurity Amendments

Sen Harper/Rep Wilcox

Expands the Cyber Center's duties to include local education agencies.

SB 183

Surveillance Camera Amendments

Sen Pitcher/Rep Teuscher

Prohibits law enforcement from tampering with an individual's surveillance camera.

SB 256

Identity Protection Modifications

Sen Cullimore/Rep Teuscher

Clarifies that defamation laws applies to content created through artificial intelligence or other technological means.

SB 267

Software in Education Amendments

Sen Cullimore

Requires the State Board of Education to create a statewide digital privacy agreement for educational software.

SB 275

State-Endorsed Digital Identity Program Amendments

Sen Cullimore/Rep Cutler

Creates the SEDI Program and authorizes the creation of a state-endorsed digital identity.

SB 290

Victim and Witness Privacy Amendments

Sen Balderree/Rep Defay

Creates restrictions on the release of a victim's nonpublic electronic data or information.

GDPA



Data Privacy Amendments

HB 450 SUB 6 - Effective 5/6/2026

63A-19-101



Specifies that a municipality's **chief administrative officer** may be a **separate** and **distinct role** from the chief administrative officer role described in Section 11-50-202.

63A-19-101. DEFINITIONS (CONTINUED)

- Defines a “**data privacy complaint**” as a complaint or concern raised by an individual regarding:
 - an alleged infringement on the individual's data privacy interests; or
 - a governmental entity's data privacy practices described in Part 4, Duties of governmental entities.
- Clarifies that **high-risk processing activities** include the use of genetic data of a living person and specific geolocation data.
- Revises the definition of “**profiling**” to mean any form of automated processing performed on personal data to evaluate, analyze, or predict an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location, or movements.
- Clarifies that “**purchase**” or “**purchasing**” does not include payment from one governmental entity to another governmental entity for access to a record.
- Revises the **definition** of “**sell**” to mean the transfer of personal data in exchange for monetary consideration by a governmental entity to a third party. This definition still provides that “sell” does not include a fee:
 - charged by a governmental entity for access to a record pursuant to Section 63G-2-203; or
 - assessed in accordance with an approved fee schedule.
- Defines “**specific geolocation data**” as information derived from technology, including global position system level latitude and longitude coordinates, that directly identifies an individual's specific location, accurate within a radius of 1,750 feet or less. (Same as defined in Section 13-61-101)

63A-19-202



Removes the requirement that the **Utah Privacy Governing Board** approve data privacy agenda items for the Utah Privacy Commission or make recommendations for additional items for the data privacy agenda.

63A-19-203



Change

Changes the composition of the Commission:

- requires the Governor to appoint a member who is a private citizen representing the public; and
- requires the State Board of Education to appoint a member who represents public education entities and the privacy interests of students.

Removal

Removes the appointment conditions for the member who represents municipalities.

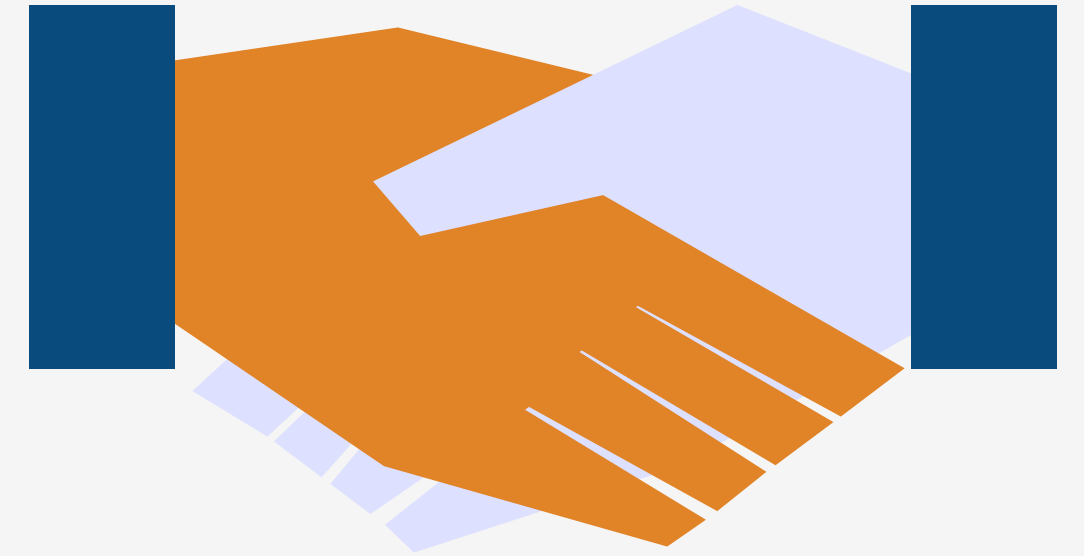
Change

Changes the provision of staff and support to the Commission from the Auditor to the Office.

Requirement

Requires the Commission to make rules establishing participation requirements for members and provides that a member may be removed if they fail to meet the requirements.

63A-19-204



Requirement

Requires that the **Commission**:

- **provide** an update and review and report on privacy developments at the request or direction of the Board; and
- **study and recommend** which information in the privacy program report should be a public record.

Removal

The Commission no longer needs to provide a data privacy agenda or annual report to the Board.

63A-19-301

Requires the Office to develop, maintain, and make available **data privacy training**, education, and awareness materials.

Allows the Office to:

- **advise the Board** about widespread or systemic data privacy matters or alleged violations;
- work with the Division of Purchasing to **develop cooperative contracts** that governmental entities **may choose** to use;
- make available privacy compliance **assessment tools** that governmental entities **may choose** to use;
- **issue guidance** or recommendations regarding compliance with the GDPA and best practices for data privacy and data governance;
- **contract** with a state institution of higher education to support the Office in:
 - conducting research and preparing reports regarding data privacy and data governance;
 - providing support to the Commission;
 - holding data governance summits and educational programs;
 - developing systems and tools to support data privacy and data governance; and
 - providing other services in support of the Office's duties;
- create **data governance models** that governmental entities **may choose** to use; and
- issue a **one-time limited extension** for governmental entities to comply with certain requirements in the GDPA.

63A-19-401



Clarifies that if a **more specific** or more **restrictive law** governs the treatment of a type of personal data, the more specific or more restrictive law **controls**.

Removes the requirement to “**document**” a non-compliant processing activity under Subsection 63A-19-401(2)(a)(iv)(B).



63A-19-401.1



Clarifies that after **July 1, 2027**, a state agency that has not completed a **privacy annotation** for a record series containing personal data, **may not** collect, maintain, or use the personal data in the record series.

63A-19-401.2

Requires employees of a governmental entity that have access to personal data, or supervise someone who has access, to complete **data privacy training** that includes instruction on:

- data privacy best practices, obligations, and responsibilities;
- the relationship between privacy, records management, and security;
- the privacy interests and requirements of this chapter; and
- as applicable, the privacy interests and requirements of GRAMA.

63A-19-401.2
(Continued.)

Data Privacy Training



Allows a governmental entity **to choose to use the data privacy training** materials created by the Office or **provide their own** data privacy training that meets the same requirements.

63A-19-401.3. Privacy Program Report.

Key change: The report **must now be shared with the Office** on or before December 31 of each year and the governmental entity must retain the report for no less than five years.

(1) On or before December 31 of each year, the chief administrative officer of each governmental entity shall prepare a report that includes:

(a) how the governmental entity has initiated the governmental entity's privacy program;

(b) a description of:

(i) the governmental entity's privacy program including privacy practices;

(ii) strategies for improving and maturing the governmental entity's privacy program and practices; and

...

(f) the percentage of the governmental entity's employees required to complete the data privacy training under Section 63A-19-401.2 that have completed the training; ...



63A-19-401.4

Pushed back the date that a new or renewed contract must have specific language regarding contractor compliance with the GDPA from July 1, 2026, to 2027.

63A-19-403

Added a requirement that a governmental entity have a procedure by which an individual may request an amendment or correction of personal data to now include "information concerning an identifiable individual contained in a record maintained by a governmental entity, **as allowed by law.**"

63A-19-405

Requires a governmental entity that identifies the unauthorized access, unauthorized acquisition, unauthorized disclosure, loss of access, or unauthorized destruction of personal data that is used or is reasonably likely to be used to commit theft, fraud, or other criminal acts to provide notification of the breach to:

- each individual whose personal data is involved in the breach; and
 - the attorney general.
-

63A-19-406

Clarifies that a governmental entity may use a contractor to send a data breach notice to an individual affected by a breach.

63A-19-407

Requires the Office and the Commission to **study** the implementation of **processing activities** for which an individual's personal data may be collected without the ability to provide direct notice:

- the **public safety benefits** and legitimate governmental purposes served by the processing activities;
- the **privacy implications** of the processing activities; and
- **appropriate frameworks** for governing the processing activities.



63A-19-408



Moves the **at-risk employee** section from GRAMA at Section 63G-2-303 to the GDPA.

63A-19-501. Data Privacy Ombudsperson

Significant revisions within the GDPA.

The revisions within the GDPA generally clarify that the Ombuds:

- Is a position within the Office.
- Serves as a resource for an individual who is making a data privacy complaint (as that term is now defined) not an open-ended complaint about any governmental entity's data privacy practice.
- **May:**
 - Mediate a dispute between an individual and an entity regarding a data privacy complaint (as detailed in the new Section 63A-19-502).
 - Provide data privacy education and training in accordance with Subsection 63A-19-301(3)(g).
- **May not:**
 - Expand the scope of a mediation beyond the data privacy complaint.
 - Mediate a dispute that is within the authority of the Government Records Office or the government records ombuds.
 - Conduct an audit of an entity's privacy practices.

63A-19-502

Complaints

Requires an individual to go directly to the chief administrative officer of a governmental entity to make a data privacy complaint instead of to the Ombuds.

Allows the Ombuds to mediate data privacy disputes if the:

- dispute cannot be resolved between the individual and the governmental entity; and
- individual or the governmental entity request mediation.

Allows an employee of a governmental entity to make a data privacy complaint to the Attorney General and provides that the employee is entitled to the protections described in Title 67, Chapter 21, Utah Protection of Public Employees Act.

SB 275. State-Endorsed Digital Identity Data Privacy Ombudsperson

Expanded duties pursuant to SB 275:

Gives the Data Privacy Ombuds the ability to receive and review complaints regarding alleged violations of Chapter 20, State-Endorsed Digital Identity, by private sector entities, and may refer such complaints to the Attorney General for enforcement.

Other Sections Affected



DTS

63A-16-108

Removes the State Privacy Auditor from the parties that DTS must consult with about digital verifiable credentials and records.

GRAMA

63G-2-601

Removes the requirement for a governmental entity to provide a notice to a person that is asked to furnish information that could be classified as a private or controlled record.

GRAMA

63G-2-601

Specifies that a governmental entity may only use the information contained in a controlled or private record for:

- the purposes described in the statement provided to the state archivist; or
- the purposes for which another governmental entity may use the record under Section 63G-2-206.

State Auditor

67-3-1

Removes the position of the State Privacy Auditor.
Added explicit language that the State Auditor may audit the privacy practices of governmental entities.

State Auditor

67-3-13

Removes the position of the State Privacy Auditor.
Changes this Section to "State auditor data privacy responsibilities."

53H-14-502



Utah Code § 53H-14-502. (Higher Education)

Enacted 2024 General Session but never implemented.

(1) The ~~state privacy auditor~~ chief privacy officer shall establish a higher education privacy advisory group to advise institutions and institution boards of trustees on student data protection.

...



Resource page

privacy.utah.gov



Laws and Regulations

[US State Data Governance Law Tracker](#)

[2026 Legislative Summary](#)

[GDPA](#)

[GRAMA](#)

[DARS Statute](#)

Stay Connected

Join the Utah Office of Data Privacy mailing list

Receive updates, resources, and upcoming training opportunities.

Share Your Success Stories

If your team has implemented a strong privacy practice, we'd love to highlight it.



UTAH OFFICE *of*
DATA PRIVACY

Contact Us

Visit us at privacy.utah.gov

or email us at officeofdataprivacy@utah.gov