



**Utah Office of
Data Privacy**

Presentation to Economic Development and Workforce Services Interim Committee

Christopher Bramwell
Chief Privacy Officer
Utah Office of Data Privacy

August 19, 2026

Utah's Government Data Privacy Framework



Government Data Privacy Act

**Privacy
Governing
Board**

**Utah Privacy
Commission**

**Utah Office of
Data Privacy**

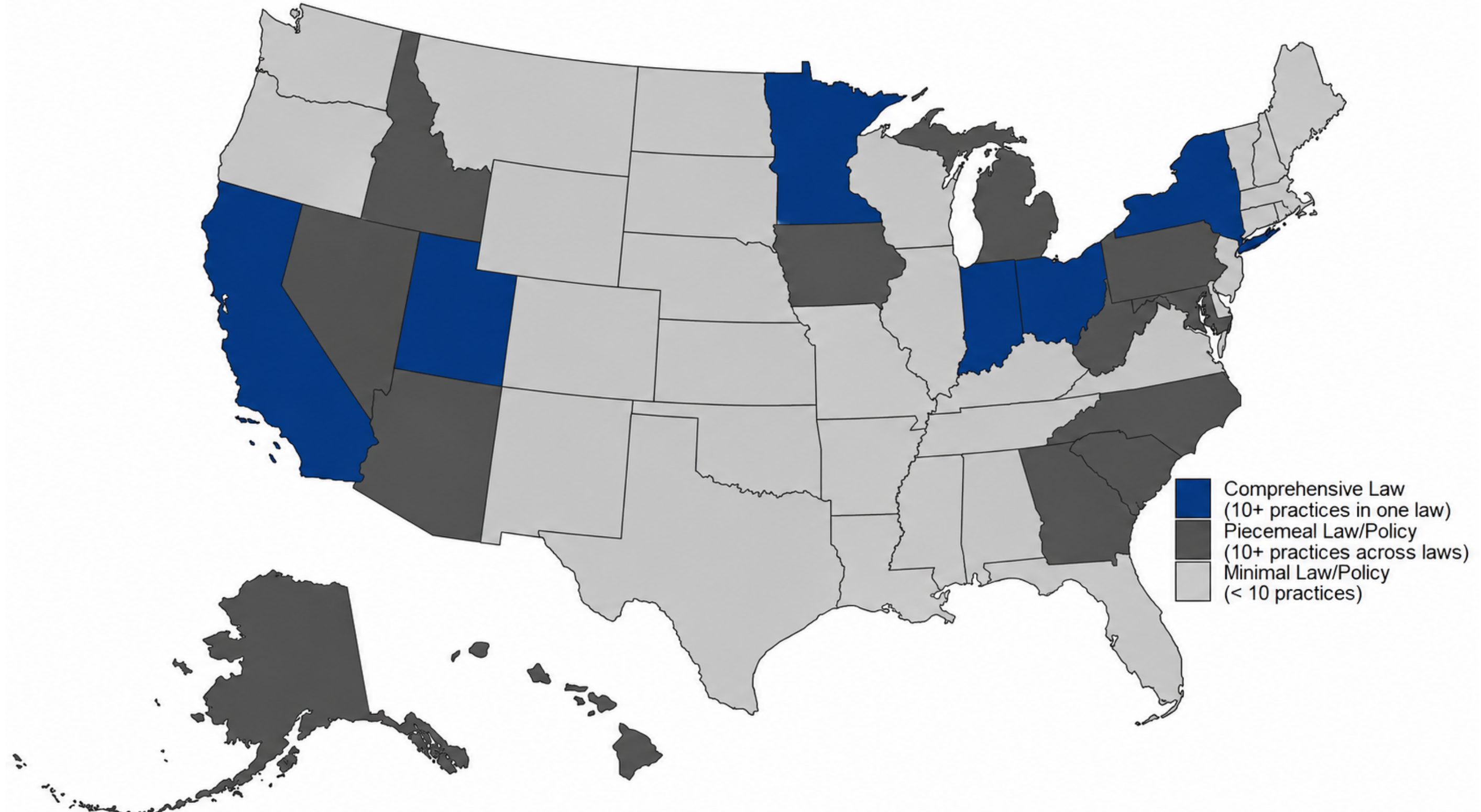
**Duties of
Governmental
Entities**

**Forward
Looking
Strategy**

**Annual
Reporting**

**Complaints and
Enforcement**

50 State Tracker Government Privacy Law



PRIVACY PRACTICES

CATEGORY	IDENTIFIER	PRIVACY PRACTICE NAME
 GOVERN	1.1	Chief Administrative Officer (CAO) Designation
	1.2	Records Officer Appointment
	1.3	Records Officer Training and Certification
	1.4	Statewide Privacy Training
	1.5	Privacy Program Report
 IDENTIFY	2.1	Record Series Creation and Maintenance
	2.2	Record and Record Series Designation and Classification
	2.3	Inventorying
	2.4	Statement Filed with State Archivist
	2.5	Retention Schedule Proposal and Approval
	2.6	Record Series Privacy Annotation
	2.7	Privacy Impact Assessments (PIA)
	2.8	Record and Personal Data Sharing, Selling, and Purchasing
 CONTROL	3.1	Data Subject Requests for Access
	3.2	Data Subject Requests for Amendment or Correction
	3.3	Data Subject Requests for an Explanation
	3.4	Data Subject Requests by At-Risk Employees for Restricting Access
 COMMUNICATE	4.1	Privacy Notice (Notice to Provider of Information)
	4.2	Website Privacy Notice and Website Privacy Policy
 PROTECT	5.1	Minimum Data Necessary
	5.2	Retention and Disposition of Records Containing Personal Data
	5.3	Incident Response and Notification to the Cyber Center and Attorney General
	5.4	Breach Notification to Affected Individuals

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

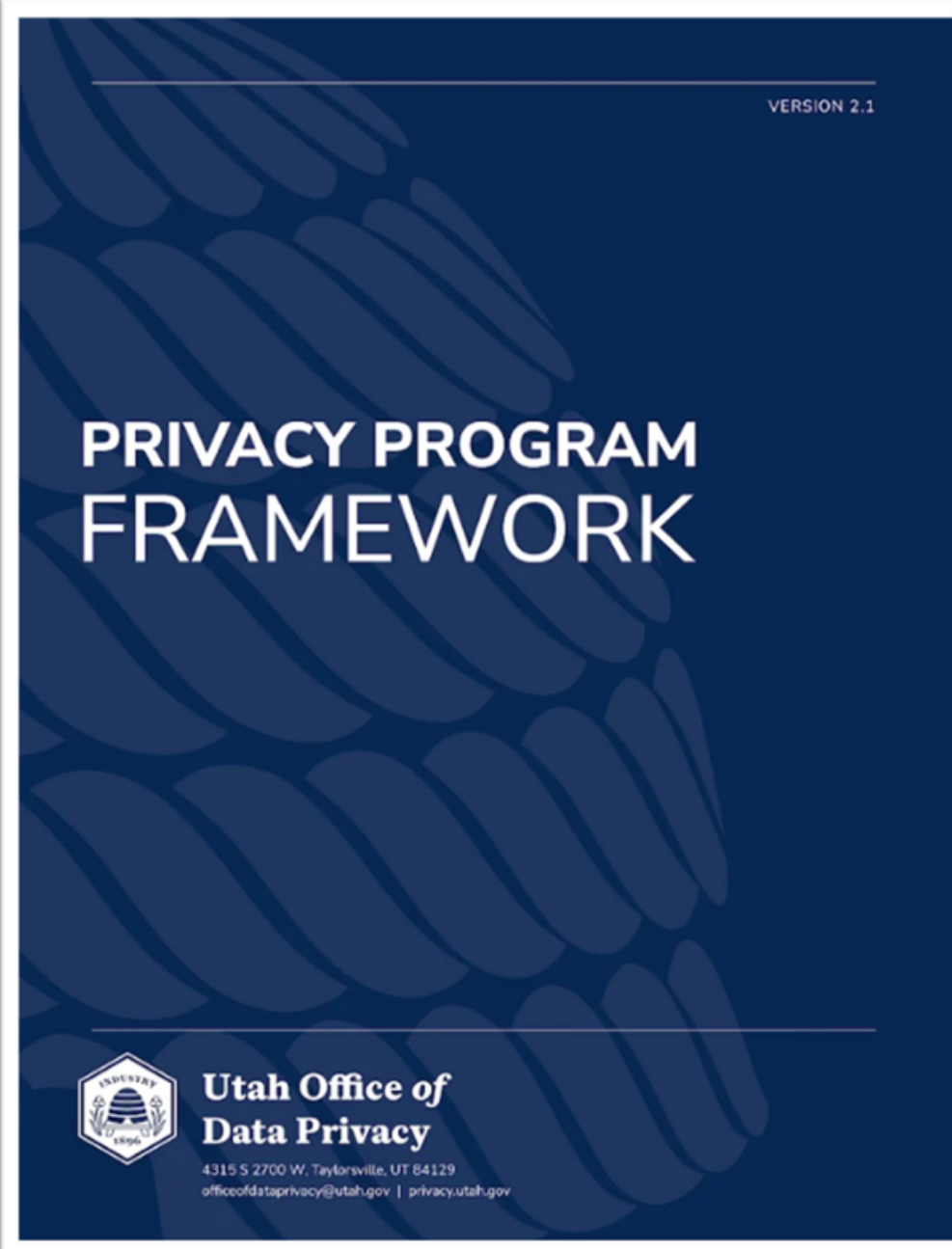
AD HOC

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.



Utah Code § 63A-19-301

Utah Office of Data Privacy Duties



- Create & Maintain a Data Privacy Framework
 - Protect personal data, ensure compliance, empower individuals, and enable lawful data sharing.
 - Adapt to each entity's resources, populations, and maturity.
- Review & Standardize Laws
 - Identify conflicts and gaps in privacy and records management statutes.
- Support Governmental Entities
 - Research best practices, remedies for non-compliance, and ways to expand individual control.
 - Focus on AI/automated decision-making, synthetic/anonymized data, and website tracking.
- Support Utah Privacy Commission

Utah Code § 63A-19-301

Utah Office of Data Privacy Duties



- Monitor & Coordinate
 - Monitor high-risk processing and develop breach response plans with the Cyber Center.
 - Integrate privacy into records management with the State Archivist.
- Training & Awareness
 - Create statewide employee data privacy training programs.
- Extensions and Exemptions
 - Approve or deny requests for extensions and exemptions to government entity privacy duties in 63A-19-401.



“Specific Geolocation Data” in Government Data Privacy Act

Utah Code § 63A-19-101

GDPA Definitions



(35) "Specific geolocation data" means the same as that term is defined in Section 13-61-101.

Utah Code § 13-61-101(33)

(a) "Specific geolocation data" means 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.

(b) "Specific geolocation data" does not include:

(i) the content of a communication; or

(ii) any data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

Utah Code § 63A-19-101

GDPA Definitions



(18)

(a) "High-risk processing activities" means a governmental entity's processing of personal data that may have a significant impact on an individual's privacy interests, based on factors that include:

- (i) the sensitivity of the personal data processed;
- (ii) the amount of personal data being processed;
- (iii) the individual's ability to consent to the processing of personal data; and
- (iv) risks of unauthorized access or use.

(b) "High-risk processing activities" may include the use of:

- (i) facial recognition technology;
- (ii) automated decision making;
- (iii) profiling;
- (iv) genetic data of a living person;
- (v) biometric data; or

(vi) specific geolocation data.

Utah Code § 63A-19 Part 4

Duties of Governmental Entities



63A-19-401(3) A governmental entity **may not**:

- (a) establish, maintain, or use undisclosed or covert surveillance of individuals unless permitted by law;
- (b) **sell** personal data unless expressly required by law; and
- (c) **share** personal data unless permitted by law.

63A-19-401.3 Privacy Program Report

- Report, including a list of all high risk processing activities, submitted to the Utah Office of Data Privacy.
- First reports will be submitted to the Office by Dec 31, 2026.

Utah Code § 63A-19 Part 4

Duties of Governmental Entities



63A-19-402 Personal Data Collection - Privacy Notice

- Government entities must provide notice at time of personal data collection which includes the purposes and uses of data. Entities are limited to those purposes and uses.

63A-19-402.5 Website Privacy Notice

- Government entities must provide notice at time of personal data collection which includes the purposes and uses of data. Entities are limited to those purposes and uses.

63A-19-404 Retention and Disposition of Personal Data

- Government entities must dispose of personal data according to retention schedules.

- What specific harms from the collection or use of specific geolocation data are we trying to prevent?
- What are beneficial government uses of specific geolocation data?
- Should government access to specific geolocation data require consent, a warrant, or other legal process?
- Is specific geolocation data obtained from a person's device their property or "papers"?
- Is specific geolocation data collected for a government service a government record under GRAMA?
- Should a government vendor ever own, license, or independently use government-collected geolocation data?
- Should protections follow specific geolocation data when it is held by vendors or other third parties?
- Should privacy protections depend on whether GDPR or UCPA applies, or should the same protections apply to the data regardless of who holds it?
- How long should government and its vendors be permitted to retain specific geolocation data?

Questions or comments



**Utah Office of
Data Privacy**

Visit us at

privacy.utah.gov

or email us at

officeofdataprivacy@utah.gov

christopherbramwell@utah.gov