OFFICE OF THE
STATE AUDITOR

State Privacy Officer Annual Report FY2024

Background:

Established in 2021, the State Privacy Officer (SPO) team supports over 1,000 designated governmental entities. Utah Code § 67-3-13-(5) requires the SPO to submit an annual report to the Judiciary Interim Committee by or on October 1 each year, detailing: the number of reviews completed, reforms made in response to reviews, reports on data sharing submitted to the SPO, and recommendations for legislation based on reviews.

During the financial year 2024 (July 1, 2023 – June 30, 2024) no formal reviews were completed and no reports on data sharing were submitted to the SPO.

The two-person SPO team prioritized conducting "**privacy health checks**" over formal reviews to measure baseline privacy maturity across entities. With the state's underdeveloped privacy landscape and limited privacy requirements before HB491 (Data Privacy Amendments), these checks provided a much-needed assessment of entities' current privacy practices and risk mitigation abilities. This fact-finding phase also helped the SPO gather key information on tools, vendors, and practices used across the state. As a result, next year's reviews will be conducted with a clearer baseline of the entities' maturity and greater entity readiness for addressing compliance with legal standards and focus on specific practices that pose the greatest risks.

Executive Summary

Our Focus

1. Systematically assessing the designated governmental entities' effectiveness in implementing adequate privacy practices.
2. Driving compliance efforts to uphold the existing privacy requirements stipulated within the Governmental Internet Information Privacy Act (GIIPA).
3. Identifying personal data over-collection, over-retention and high-risk activities, with focus on reviewing online tracking and personal data collection points.

Our Results

→ The SPO conducted **32** individual privacy health checks: 31 entities found at **ad-hoc level**, one at **non-existent** privacy program maturity level.

→ Compared to FY2023, website privacy policy statement compliance improved by over **20%** due to rigorous work of the SPO with the entities.

→ **71** entities were found collecting double or more trackers than the national average. High risk activities found to be mostly unidentified and unmeasured by the entities.

4. Providing expertise leading up to and during the legislative session to reduce privacy risks for Utah residents.	→ The SPO reviewed **66** privacy bills and provided significant contribution to the drafting of Government Data Privacy Act (GDPA).
5. Raising privacy awareness among the entities as well as Utah residents.	→ The SPO held **27** training sessions for over **1,600** participants.
6. Driving the efforts to greater compliance with the Government Records Access and Management Act (GRAMA) through records management sessions.	→ The number of records officers with active certification has increased by **225** additional individuals obtaining certification compared to FY2023.

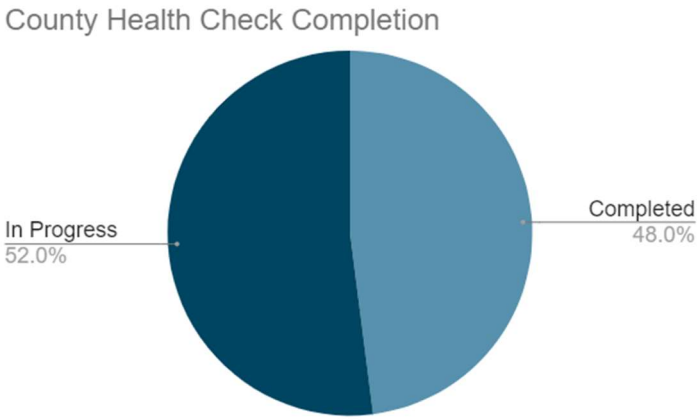
Key Gaps Identified:	**Solutions Provided by the SPO**
1. Inadequate employee training on privacy practices, leading to a lack of awareness.	1. Created new-hire training for entities to implement immediately.
2. Poor vendor vetting for personal data access and inadequate contract management processes.	2. Created a template of vendor privacy clauses and guidelines for contract management.
3. Non-existent or insufficient monitoring metrics for measuring privacy compliance, risk levels and progress made.	3. Created and published compliance monitoring metrics for the entities to use to measure risk and progress.
4. Lack of inventory of personal data and data sharing practices.	4. Created and disseminated a personal data inventory template for entity use.
5. Inconsistent encryption standards often leaving out legacy devices and external email communication.	5. Recommended that entities include legacy devices and email communication in encryption standards.
6. Inadequate Incident Response Plans and lack of Data Loss Prevention (DLP) tools used within entities.	6. Delivered basic steps to incident response and worked with the Cyber Center to disseminate their materials.

Annual Report Details

SPO Achievements

1. **Privacy Health Checks:** the SPO reviewed **32** entities throughout the year. 31 out of 32 entities were assessed as having an "**ad-hoc**" approach to mitigating privacy risks. This was characterized by the lack of a dedicated privacy function and program, no systematic training, and the absence of a comprehensive privacy policy. Instead, these entities followed ad-hoc rules or processes that were not fully codified. Administrative, technical, and physical safeguards were reviewed, with the largest gaps identified in administrative safeguards.

   Technical safeguards were resource-dependent; while entities were aware of the need to enhance personal data protection, they often struggled to secure adequate resources. Additionally, entities were found to lack a thorough understanding of their data collection and sharing practices. This was highlighted as a key priority for most of the assessed organizations to address first, to minimize data collection and adequately protect the data collected.



How are privacy health checks done?

1. SPO conducts on-site visits to designated governmental entities, meets with a group of five to ten preselected individuals from teams responsible for processing personal data for a two-hour risk assessment.
2. In the meeting, the entity's ability to protect personal data is discussed and effectiveness as well as awareness are measured through real-time group interviews and a site review.

3. SPO then produces a high-level report assessing the organizational privacy maturity level and recommends concrete steps to bridge identified gaps, including timelines and highlighting top risks for focus.
4. SPO provides the Privacy Toolkit, which includes templates and other tools, as part of each health check.
5. SPO reviews new policies and processes as part of the follow-up and provides targeted training.

Success Story

St. George has emerged as an outstanding champion for data privacy through the efforts of its legal office. The City's legal office works with various city departments, such as HR, administrative services, and others. They led the way in driving significant improvements in privacy practices across the organization. After conducting a Privacy Health Check through our Office, the City recognized gaps in their data collection practices, prompting them to act swiftly. The legal office, under the direction of Assistant City Attorney, Alicia Carlton, implemented a privacy notice for the city's website. The legal office and IT department collaborated with the Human Resources Department to initiate employee privacy training.

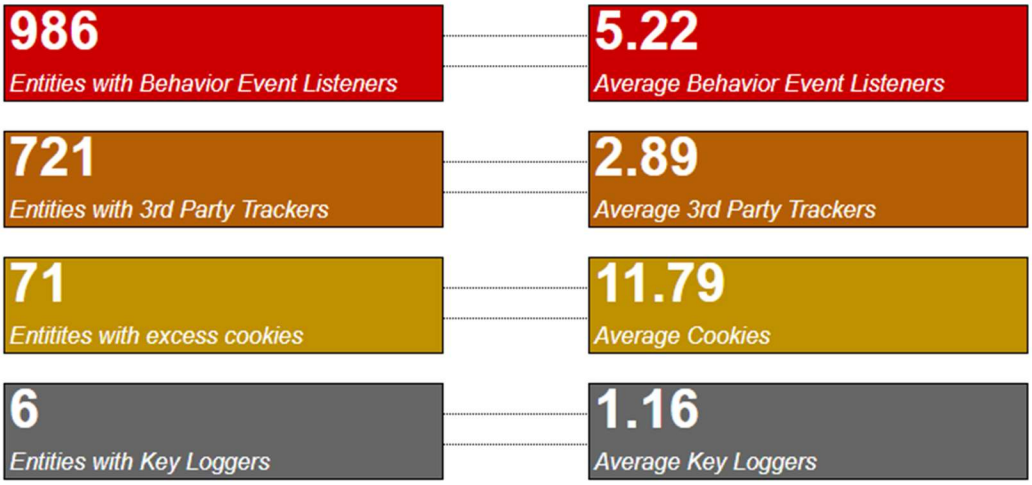
Carlton emphasizes the importance of an ongoing commitment to privacy, describing it not just as a technical issue, but a mindset that needs continuous education and adaptation. By fostering this culture, St. George strives to make data privacy a central part of its public administration, ensuring that it's not just a legal concern, but an organizational practice embedded throughout the city's services.

St. George received the Excellence in Privacy Engagement award from the State Privacy Officer.

2. **Training**:
    - SPO conducted **27** individual training sessions with target audiences from education, law enforcement, counties, towns, cities, and special districts. Sessions spanned from small, in-person groups to large, online groups. Many of these sessions were also open to both state and national participants.
    - Training reached an overall audience of over **1,600** unique participants.
    - SPO founded a **Privacy Academy** and planned its first run as a seven week-long course starting October 2024, covering seven modules, 90 minutes each, focusing on the most pressing privacy topics such as breach notification, Privacy Impact Assessment (PIA) Use, and prevention of over collection and over retention of data. The academy got the accreditation of the Utah Supreme Court Board of Continuing Education to offer Continuing Legal Education credits to participating legal counsels.

3. **Website Review:**
    - SPO conducted a sweep of over 1500 websites of governmental entities (this includes non-profits), to review existence of privacy policy statement, as required by the Governmental Internet Information Privacy Act (GIIPA).
    - We also conducted a privacy scan of these entities' websites to identify the number of cookies, trackers, and advertising beacons, as well as key loggers and behavioral listeners.
    - During these exercises we uncovered websites that were not managed by the entities, or the entities didn't realize that personal data was collected through their websites. We worked with these entities individually to remedy these risks.

Results of the Privacy Scan of Entities' Websites



4. **High-Risk activities:**
    - SPO is mapping the use of AI throughout local law enforcement, with special focus on the use of generative and predictive AI.
    - SPO provided guidance to all counties and cities that have participated in the privacy health checks, as well as to additional entities who requested it.
    - SPO developed a Privacy Impact Assessment (PIA) template, trained selected entities on its use to address high-risk data processing, and conducted two PIAs.

5. **Policies:**
    - SPO created and published a **Privacy Toolkit** including privacy guidelines and 12 templates for policies addressing protecting personal privacy throughout data lifecycle.
    - We reviewed **137** individual privacy policy statements for designated governmental entities and provided guidance on implementation with a focus on transparency and data minimization.

6. **Videos:** Created and published three educational videos:
    - Privacy for New Hires
    - Privacy Policy Statement
    - Privacy Policy Implementation

7. **Newsletter:** Developed and published a Monthly Privacy Newsletter, with an audience of **1062** recipients, addressing current topics such new laws coming into effect or new training opportunities offered.

8. **Privacy Alerts:** Launched privacy alerts, published on the Office of the State Auditor website. Topics published in FY 2024: Risk of using generative AI, Preventing AI powered scams.

9. **Impact Survey:** Conducted an impact survey sent to over **1300** participants from both state agencies as well as designated governmental entities. Community feedback indicated that respondents implemented many recommendations based on the training and health checks conducted.

Participants mentioned they implemented:

- Holistic privacy policies, privacy statements, privacy notices, incident response plans, data inventories, standardized vendor clauses addressing privacy, improved technical safeguards and breach notification processes as well as additional trainings, and reviews of data collection and data destruction points.
- Mapping of their data repositories and data sharing practices, in order to be able to fulfill a Government Data Privacy Act (GDPA) requirement to submit annual report on data sharing.

Participants asked for additional support on:

- Training, including more in-person sessions, with additional courses targeting specific topics related to the Government Data Privacy Act (GDPA).

- Some participants expressed frustration with the complex burden of the new legal requirements, especially for the smallest municipalities that do not have adequate bandwidth and/or expertise.
- More public outreach and communication toward participants.
- Assistance with customizing the provided templates, as well as a request for supporting grants and identifying additional funding.
- Training for the leaders and decision makers, to secure adequate resources and support in obtaining needed expertise.
- In-depth training on data minimization and retention (46%) and privacy program development (42%). There was also significant interest in training on the Government Data Privacy Act (44%) and AI data privacy risks (35%). Technical topics like Mobile Device Management (MDM) and Multi-Factor Authentication (MFA) were less of a priority.

2024 Legislative Session Support

The SPO reviewed 66 bills during the legislative session. This was done to analyze impact on personal privacy, to lend expertise to the legislators and drafting attorneys as needed, and to advocate on behalf of Utah residents throughout the session. Full list of these bills is in attachment E of this report.

These following bills were of particular interest to the SPO:

HB 491: The SPO and the State Auditor played a key role in shaping this bill. The SPO team has been actively training entities since its passage. We are proud to have ensured an effective wording on the ban of sale of personal data, the annual privacy training requirement, and a clear definition of personal data aligned with national and global standards. During the legislative session, the SPO raised concerns about the immediate impact on designated governmental entities, suggesting a 12–24-month grace period for most requirements, except breach notification, due to the limited resources of the small to medium size entities. However, the bill took effect in May 2024 as the Government Data Privacy Act (GDPA) with most requirements already, and many entities are struggling to comply, as reflected in our impact survey.

HB 118: SPO noticed a terminology concern with potential constitutional impact in this bill prior to the first house reading. The concern was raised with the drafting attorney, the Utah privacy commission (UPC), as well as legislators. SPO also enlisted the assistance of a leading expert on digital identity (member of UPC). The SPO recommended changes will be addressed during the upcoming legislative session.

HB 257: In reviewing this bill, SPO raised a concern that the bill tasks schools with effectively collecting and maintaining some of the most sensitive data related to students such as gender identity and healthcare. SPO cautioned against the over collection of personal data.

HB 135: SPO worked with the drafting attorneys on clarification of this bill that significantly limits the ability of Utah governmental entities of using drones that were assembled or manufactured outside of the USA. SPO consequently provided relevant training to the governmental employees.

Records Management Metrics

The SPO continues to drive improved compliance with the Government Records Access and Management Act (GRAMA) requirement to have designated and fully certified Records Officers throughout all local governmental entities.

Certified Records Officers Metrics

Table 1: Summary of entities with a listed Records Officer by entity type sorted by rate of change.

Entity Type	FY2023	FY2024	% Change
Local District	4	25	**525%**
College or University	26	55	**111%**
County	238	486	**104%**
Interlocal	18	31	**72%**
Associations of Government	7	12	**71%**
Independent or Quasi-Government	9	15	**66%**
Municipality	441	728	**65%**
Charter School	122	197	**61%**
Special Service District	425	679	**59%**
Public School	214	277	**29%**
Other	8	9	**12%**

Table 2: Summary of entities with active Records Officer certifications by entity type, sorted by rate of change.

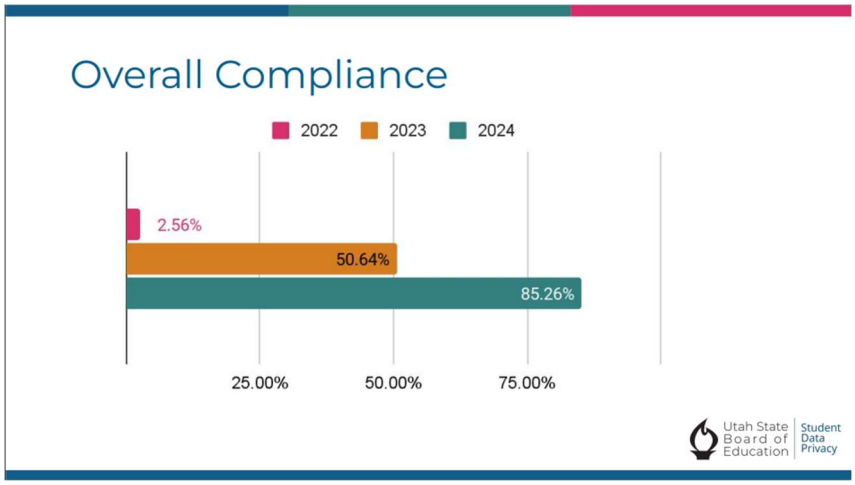
Entity Type	FY2023	FY2024	% Change
Local District	3	22	**633%**
Associations of Government	5	9	**80%**
College or University	24	37	**54%**
County	180	271	**50%**
Municipality	377	495	**31%**
Independent or Quasi-Government	7	9	**28%**

Charter School	101	117	**15%**
Interlocal	19	18	**-5%**
Public School	138	129	**-6%**
Special Service District	339	315	**-7%**
Other	10	6	**-40%**

Utah State Board of Education (USBE) - Education Privacy Metrics

USBE tracks the use of the following documents: Annual notice of the Family Educational Rights and Privacy Act (FERPA), Directory Information Notice, Student Data Collection Notice, and Data Governance plan.

The following general compliance metric captures improvement between FY2023 and FY2024 as provided by the Utah State Board of Education (USBE). USBE is a frequent collaborator with the SPO and has also undergone a privacy health check in FY 2024.



FY2025 SPO Goals

1. Conduct at least two reviews, prioritizing the use of generative and predictive AI tools within selected law enforcement entities.
2. Continue to drive increased compliance with the Governmental Internet Information Privacy Act (GIIPA) by another 20% or more, moving general entity compliance over 75%.
3. Complete health checks for the remaining 52% of counties, and at least five large municipalities.

4. Increase public outreach within the entities as well as public. Increase number of subscribers to the SPO newsletter by at least 10%.
5. Continue collaboration with law enforcement to explore the potential uses and implementation of AI. Document both positive feedback and concerns.
6. Conduct at least 10 Privacy Impact Assessments (PIA) for high-risk activities. After a phase dedicated mainly to fact finding, discussions, documentation, we will provide systematic support in implementing PIAs and addressing high risk activities.
7. Utilizing our developed Privacy Toolkit and insights gained from Privacy Health Checks, assist local governmental entities in effectively implementing their privacy programs per their request.
8. Continue to work on data minimization efforts through work with entities to review their data collection and data sharing points as well as lowering the number of cookies and trackers to levels at or below national average with a focus on addressing covert surveillance.
9. Deliver privacy related trainings, as requested, on topics such as: Government Data Privacy Act (GDPA), AI use, Privacy 101, and more.
10. Address limited scalability of SPO provided services: SPO requested three additional FTEs to assist in reviewing and implementing requirements from the GDPA. If approved, this will also significantly help with increasing SPO's impact and entity outreach initiatives as well as conducting reviews.
11. Continue to treat privacy as a basic human right and draft language for Utah constitution that would reflect it and strengthen the right to privacy.
12. Continue to educate governmental employees on privacy rights of Utah residents.
13. Strengthen awareness of OSA hotline.
14. Encourage legislators to strengthen protection of whistleblowers and collaborate to draft language as needed.
15. Provide privacy policy expertise as a resource to drafting attorneys of the Office of the Legislative Research and General Counsel (OLRGC), with special focus on further improving of the Government Data Privacy Act (GDPA) and HB118.

Conclusion

In FY2024, the SPO's health checks revealed systemic and widespread deficiencies in privacy practices across designated governmental entities, particularly in their ability to inventory and classify personal data and map data sharing processes. These findings underscore the need for continued focus on identifying high-risk data processing. Given limited resources, this initial phase of assessing baseline privacy maturity was critical for understanding the landscape and uncovering the most significant weaknesses in process. As privacy requirements continue to evolve with the full implementation of the Government Data Privacy Act (GDPA), future efforts should prioritize review of high-risk activities to strengthen compliance across the state.

LIST OF APPENDICES

- Appendix A. Entity Overview
- Appendix B. Authorities of the Utah Privacy Program
- Appendix C. Training and Awareness Sessions
- Appendix D. Privacy Maturity Levels
- Appendix E. 2024 Legislative Review
- Appendix F. Monitoring Recommendations
- Appendix G. Local Education Agency Privacy Compliance Requirements

Appendix A. Entity Overview

As of September 2024, the in-scope designated governmental entities included:

- 269 Local and Special Service Districts
- 155 School Districts or Charter Schools
- 148 Cities
- 124 Law Enforcement Agencies
- 107 Towns
- 77 Redevelopment Agencies/Project Areas
- 57 Interlocal entities
- 35 Conservation Districts
- 37 Components
- 29 Counties
- 21 Educational Foundations
- 16 Housing entities
- 18 Institutions of Higher Education
- 14 Independent/Quasi State Entities
- 7 Associations of Government
- 2 Community Reinvestment Agencies
- 2 District Health Departments
- Utah State Board of Education
- Office of the State Auditor
- Office of Attorney General
- Office of State Treasurer
- Office of Legislative Research and General Counsel

1,123 Total Entities

Appendix B. Statue and Administrative Rules of the Utah Privacy Program

- Government Data Privacy Act
  Utah Code § 63A-19-101 et seq.
- Division of Archives and Records Services (AKA Public Records Management Act (PRMA))
  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.
- Government Operations Privacy Officer
  Utah Code § 67-1-17
- Utah Privacy Commission
  Utah Code § 63C-24-101 et seq.
- State Privacy Office
  Utah Code § 67-3-13
- Unauthorized Access to Information Technology
  Utah Code § 63D-3-101 et seq. (Part 1 - Computer Abuse Data Recovery Act)
- Utah Technology Governance Act. Chief Information Officer
  Utah Code § 63A-16-210 Chief Information Security Officer
- Utah Technology Governance Act. Data Security Management Council
  Utah Code § 63A-16-701--702
- 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 Transparency Advisory Board
  Utah Code § 63A-18-101 et seq.
- Cybersecurity Affirmative Defense Act
  Utah Code § 78B-4-701 et seq.
- Utah Geographic Information Systems Advisory Council
  R895-9 et seq.
- Uniform Electronic Transactions Act
  Utah Code § 46-4-101 et seq.

- Electronic Records in Government Agencies
  Utah Code § 46-4-501--503
- Public School Data Confidentiality and Disclosure
  R277-487

Appendix C. Training and Awareness Sessions

FY 2024 Conducted trainings

- Explore Your Digital Footprint - July 13, 2023
- Privacy Vendor Clauses - August 2, 2023
- Breach Reporting - September 13, 2023
- Airport Law Enforcement: Ethical Use of AI - September 26, 2023
- Wasatch County Dept. Heads: Privacy 101 - September 26, 2023
- Wasatch County Sheriff's Office: Privacy 101 - October 24, 2023
- Wasatch County IT: Privacy 101 - November 2, 2023
- Privacy Risk Mitigation - November 16, 2023
- Privacy Policy Statement - November 29, 2023
- Privacy Training for Utah Government Leaders - January 9, 2024
- All Scams and 2024 Legislation - March 6, 2024
- Government Data Privacy Act for Leadership - April 30, 2024
- Treasurers: Privacy 101 - May 1, 2024
- IT Directors Government Data Privacy Act Overview - May 1, 2024
- Government Data Privacy Act - May 22, 2024
- Utah Safety Summit: Curb Your AI - June 12, 2024
- Privacy 101 for Recorders - June 13, 2024
- Bar Association: Government Data Privacy Act - June 17, 2024

FY2025 Conducted trainings up to date of submission of report (October 1, 2024)

- Tooele County: Privacy 101 - August 5, 2024
- Utah Drone Regulation - August 14, 2024
- Orem Water District: Annual Privacy Training - August 16, 2024
- Ethical Use of AI - August 21, 2024
- Generative AI Plus New Hires Training - August 27, 2024
- Government Data Privacy Act (HB 491) - September 4, 2024
- Government Data Privacy Act - September 5, 2024
- Whistleblower Protection - September 12, 2024
- Privacy 101 - September 27, 2024

Upcoming

- Privacy & HR - October 2, 2024
- Privacy 101 - October 24 & 29, 2024
- Privacy 101 - October 29, 2024
- Ethical Use of AI - October 30, 2024
- Privacy Academy - October 14 - December 3, 2024

Appendix D. Privacy Maturity Levels

Non Existent:

Non-existent or undocumented privacy officer role, and undefined privacy leadership structure. No centralized oversight or specific accountability for ensuring the privacy principles are adhered to. Where a privacy management function exists, communication between the privacy officer/privacy management function and other parts of the agency is limited.

No consideration for or integration of privacy management in strategy planning. No defined tolerance levels in relation to individual privacy risks. No consideration for privacy strategy by the governance board and/or committee(s), and/or the executive leadership team.

No guidelines or codified policies on privacy exist.

Ad-Hoc:

Privacy officer/ privacy management function responsibilities exists at least partially. Privacy/ Records management officer's role mainly consists of meeting the requirements of applicable laws, e.g., dealing with privacy disclosures and complaints. Communication between privacy officer and other parts of the agency largely occurs in response to breaches.

Privacy program does not exist or is not comprehensive and/or operationalized throughout the agency. Policies are largely uncodified, or obsolete/not periodically reviewed, with some missing. Where there is a privacy policy or standard, its implementation is not properly documented.

None or minimal monitoring and testing function or tasks are performed to review privacy compliance. None or ad-hoc metrics on privacy maturity collected. Risk appetite unclear, inherent versus residual risk not routinely measured.

Repeatable:

Privacy officer/privacy management function oversees a privacy work and Privacy program and maintains central oversight of privacy initiatives and activities on an agency-wide basis. Privacy officer/privacy management function communicates regularly with other "second-line-of-defense" functions (e.g., records management, security, risk management).

Privacy policies exist and have been distributed across the organization. Some of the processes described in them are repeated regularly. Risk baseline has been measured.

Privacy program exists and includes some monitoring metrics, but is only partially implemented.

Managed:

Privacy officer/privacy management function routinely contributes to process design and risk assessment. Privacy officer/privacy management function has established ongoing

communication and clear alignment (where applicable) with the work programs of other second-line-defense functions.

Results of privacy risk assessments are used to inform and update the privacy strategy and plan. Governance board/committee(s)/executive leadership team know what risk appetite means in relation to privacy and to the objectives and strategies set by executive management.

Optimized:

Privacy officer/privacy management function is responsible for the operational and strategic elements of privacy management on an agency wide basis. It also has the capability, capacity, and authority to introduce and implement privacy management better practices. Second-line-of-defense function proactively approaches the privacy function for input to their work programs. This communication is open, honest, and ongoing.

Privacy considerations are integrated into the overall strategy. Periodic Risk assessments are firmly embedded into the privacy program. Information obtained through risk assessment or review of response to any identified breach is used to inform updates to the privacy strategy.

All staff and contractors are responsible for privacy management and consider it normal practice to identify opportunities for improvement. Leadership work collectively and visibly to seek innovative ways to continuously improve privacy management. Managers and leaders are committed to making privacy core to the culture through their visible actions, planning, and decision making. Staff and management are comfortable identifying areas for improving privacy practices and discuss/raise these freely and proactively.

Reporting is formalized and sent to all appropriate levels of the entity, including senior leadership. The agency's privacy key performance indicators are used to track and measure organization-wide privacy performance. These indicators are used to drive all aspects of organizational privacy management improvement.

The Privacy program is robust, routinely reviewed, includes template language and risk assessment tools, and has been fully implemented and operationalized and tested within the agency

Appendix E. 2024 Legislative Review

Reviewed and Passed Legislation

The SPO reviewed the following bills during the legislative session, to analyze privacy impact and to lend expertise to the legislators as needed and to advocate on behalf of Utah residents throughout the session.

- HB010 Public Fund Amendments
- HB012 Tax Incentive Revisions
- HB013 Infrastructure Financing Districts
- HB014 School Threat Penalty Amendments
- HB015 Criminal Code Recodification and Cross
- HB016 Sexual Offenses Amendments
- HB021 Criminal Accounts Receivable Amendments
- HB030 Road Rage Amendments
- HB050 Aggravated Assault Modifications
- HB059 Federal Funds Contingency Planning
- HB069 DUI Testing Amendments
- HB072 State Boards and Commissions Amendments
- HB080 Conflict of Interest Disclosure Modifications
- HB082 Public Education Program Modifications
- HB086 Public Safety Data Amendments
- HB087 Department of Government Operations Revisions
- HB110 Sex and Kidnap Offender Registry Amendments
- HB118 Prohibition of Production of Private Keys
- HB147 Threat of Violence Amendments
- HB172 Immigrant Student Athlete Participation
- HB182 Student Survey Amendments
- HB212 Vital Records Amendments
- HB213 Crime Victim Records Amendments
- HB225 Unlawful Kissing Of A Child
- HB234 Vital Record Information Modifications
- HB248 Inmate Amendments
- HB257 Sex-Based Designations For Privacy, Anti-Bullying, and Women's Opportunities
- HB259 Juvenile Interrogation Modifications
- HB261 Equal Opportunity Initiatives
- HB316 Inmate Assignment Amendments
- HB319 Exchange of Clinical Health Information Amendments
- HB328 Victims of Sexual Offenses Amendments

- HB352 Amendments to Expungement
- HB491 Data Privacy Amendments
- HB538 Protection of Elected Official Personal Information
- SB023 Offender Registry Amendments
- SB024 Physician Assistant Practice Amendments
- SB044 Alternative Education Scholarship Combination
- SB046 Health and Human Services Amendments
- SB076 Evidence Retention Amendments
- SB088 Juvenile Justice Amendments
- SB089 Social Media Modifications
- SB098 Online Data Security and Privacy Amendments
- SB104 Children's Device Protection Act
- SB228 Protective Order Amendments
- SB231 Public Surveillance Prohibition Amendments
- SB246 Juvenile Justice Modifications

Reviewed Legislation That Did Not Pass

- HB027 Criminal Code Amendments
- HB127 Bars Incident Reporting
- HB139 Mental Health Treatment Study
- HB150 Aggravated Assault Amendments
- HB162 Sexual Offense Amendments
- HB201 Traffic Enforcement Amendments
- HB307 Firearm Data Amendments
- HB309 Driver License Amendments
- HB329 Artificial Intelligence In Political Advertising
- HB342 Electronic Information Privacy Amendments
- HB349 Personal Identifying Information In Government Records
- HJR012 Proposal To Amend Utah Constitution - Public Education System
- HJR012 Joint Resolution On the Illegal Immigration Crisis
- SB105 Student Privacy and Modesty In Public Education
- SB218 Genetic Genealogy Amendments
- SB232 Minor Data Protection Amendments
- SB271 Expungement Changes

Appendix F. Monitoring Recommendations

1. Privacy Policy and Notices

A government entity has updated Privacy Policy Statements and Privacy Notices (at data collection), which undergo yearly updates and are available to the public.

Metrics to measure:

1. Designated government entity has a privacy policy on their website - Yes/No
2. Such policy has been reviewed/updated within the last 12 months - Yes/No
3. Such policy complies with legal requirements outlined in code - Yes/No
4. Designated government entity embeds privacy notices at entry points of data collection - Yes/No
5. Such notices are periodically (at least annually) reviewed for accuracy - Yes/No

2. Regular Health Checks

A government entity conducts regular checks to assess compliance with privacy policies and procedures. Recommended frequency is annually. Audits or health-checks can identify areas of noncompliance and help designated government entity takes corrective action to ensure that privacy policies are being followed.

Metrics to measure:

1. Health-check conducted - Yes/No,
2. Outcome shows improvement since the last check was performed – Yes/No

3. Incident Tracking

A government entity tracks privacy incidents and data breaches. By tracking incidents, designated government entities can identify patterns and trends that may indicate weaknesses in privacy policies and procedures.

Metrics to measure:

1. Incident tracking is being done - Yes/No
2. Trends of reported incidents show raise of awareness (reported numbers are not zero in more than one measured consecutive period) - Yes/No
3. Root-cause analysis is being performed - Yes/No
4. Ratio of incidents vs breaches is bigger than 1:1 - Yes/No
5. Lessons learned are implemented - Yes/No

4. Privacy Training

A government entity provides privacy training to employees to ensure that they understand the importance of privacy policies and know how to follow them. Ongoing training helps employees stay up-to-date on changes to privacy policies and procedures.

Metrics to measure:

1. Mandatory privacy specific training for is assigned to all new hires - Yes/NO
2. Mandatory training extends to vendors and volunteers - Yes/No
3. Annual mandatory training that is privacy specific is provided to all employees - Yes/No

4. Records of completion/attendance of all trainings is kept - Yes/No
5. Training modules get updated annually to reflect new changes in best practices and laws Yes/No
6. Additional trainings (especially role specific or law specific) is provided on regular basis Yes/No

5. Privacy Impact Assessments (PIAs)

A government entity conducts PIAs to identify potential privacy risks associated with new projects or initiatives. PIAs can help designated government entities design privacy safeguards that are built into new systems or processes from the outset.

Metrics to measure:

1. Number of PIAs conducted is >0 for measured period - Yes/No
2. PIA conducted for each project involving a large amount (over 100 000 data elements) of data - Yes/No.
3. Conducted PIAs records kept for at least 3 years from the date the PIA was conducted Yes/No

6. Internal Reporting

A government entity encourages employees to report any privacy incidents or concerns to the designated government entity's representative or SPO. This can help entity identify potential areas of non-compliance and take corrective action.

Metrics to measure:

1. Designated government entity has a dedicated Privacy/ Records Management Officer- Yes/No
2. Such officer has undergone specific training /obtained certification for their role - Yes/No
3. Designated government entity has several avenues dedicated to incident reporting - Yes/No

7. Privacy Rights

A government entity is able to respond to data subject requests and furnish their rights, such as right to access, correct or delete their personal data. Due responses help build trust in government.

Metrics to measure:

1. Individual Request Response time measured - Yes/No
2. Majority of Data Subject Request Response time within a legislated time frame - Yes/No
3. Response time improved since last period metrics were collected for - Yes/No

8. Privacy Complaints

A government entity tracks privacy complaints, analyzes root cause and embeds appropriate safeguards based on findings.

Metrics to measure:

1. Designated government entity tracks number of complaints per year - Yes/No

2. Overall number of substantiated complaints is smaller than last measured period or corresponds with extra activities to raise awareness about complaint process - Yes/No
3. All complaints have been resolved and complainant informed on results - Yes/No
4. Time to resolve complaints is tracked - Yes/No

9. Records Retention Schedules

A government entity periodically reviews their adherence to respective records retention schedules, practices clean desk exercise and has an updated policy on records management and data classification.

Metrics to measure:

1. entity conducts an annual review of obsolete records - Yes/No
2. entity undertakes steps to establish record classification standard - Yes/No
3. entity includes records management in yearly mandatory training - Yes/No
4. entity submits necessary documents to the State Archives per respective code section - Yes/No
5. Records Officer certification is in compliance at time of check – Yes/No

10. Third Party Management

A government entity adequately manages its vendors that may have access to the entity's data, stores underlying documents properly and monitors compliance.

Metrics to measure:

1. Repository of contracts exists - Yes/No
2. Contracts include appropriate privacy clauses, vetted by legal counsel - Yes/No
3. At the end of the relationship the vendor is required to produce certificate of destruction of data - Yes/No
4. Owner of the relationship has been clearly assigned - Yes/No

Appendix G. Local Education Agency Privacy Compliance Requirements

Local education agencies are required to follow the below listed requirements:

One Time	
Develop the following policies	
Create a data governance plan	53E-9-301(7)
Work with parents to create a PPRA policy	20 USC 123h(c)
Beginning of Year	
Provide the following notices to parents	
Annual FERPA Notice	34 CFR 99.7
Directory Information	34 CFR 99.37
Military Recruiter/Institution of Higher Education notice (often included in Annual FERPA Notice)	20 USC 7908
Notice of record exchange after school transfer (often included in Annual FERPA Notice)	34 CFR 99.34
Collection Notice	53E-9-305(2)
PPRA notice (must be given by hand, mail, or email)	20 USC 1232h(c)(2) 53E-9-203(4) - (5)
Throughout the year	
Provide annual training to all staff that have access to student education records on federal and state privacy laws	53E-9-203
Ensure that data is collected in accordance with your collection and survey notices	53E-9-305 53E-9-203 20 USC 1232h
Ensure that parent and eligible student rights to access, seek to amend, and consent to disclose are followed	34 CFR 99, subparts B, C, and D
Ensure that all disclosures of student data follow FERPA, the contract requirements of the SDPA, and your data governance plan	34 CFR 99, Subpart D 53E-9-308 53E-9-309
Update your metadata dictionary	53E-9-303

Abbreviations used:
FERPA - Family Educational Rights and Privacy Act
PPRA - Protection of Pupil Rights Amendment