OFFICE OF THE
STATE AUDITOR

State Privacy Officer Annual Report

October 1, 2023

Office of the State Auditor

Whitney Phillips, PhD, State Privacy Officer
Nora Kurzova, JD, Assistant State Privacy Officer

Table of Contents

Executive Summary

Introduction

Utah Code § 67-3-13 requires the State Privacy Officer (SPO) to submit an annual report to the Judiciary Interim Committee on or before October 1 of every calendar year. The SPO is a function established in 2021. This office supports over 1,600 designated government entities. For an overview of the entities see Appendix A. For an overview of authorities and legislation affecting the Privacy Program see Appendix B.

FY2023 State Privacy Officer Goals

The SPO follows goals outlined in Utah Code § 67-3-13 which include:

- Risk classification,
- Compliance monitoring,
- Recommendations for improvement, and
- Training and awareness initiatives.

Due to the limited size of the SPO team, the first priority was to classify entities by risk to allocate resources effectively to the entities posing the highest risk and evaluate their privacy maturity.

Findings

Reviewed and interviewed entities show immature or nonexistent privacy programs—some entities have gaps with unmitigated inherent privacy risk and other entities having poorly mitigated residual risk. No entities were found to have an optimized privacy program or well-managed privacy practices.

However, the education sector stood out as more advanced with privacy policies and implemented processes being more prevalent. This is partially due to the federal obligations arising out of The Family Educational Rights and Privacy Act (FERPA), and partially due to the sector having an education specific state privacy law with funding to create privacy resources and measure maturity across 150 districts and charter schools in previous years.

Key General Gaps Identified

- Over-collection and over-retention
- Lack of data inventories
- Lack of and/or inconsistent training opportunities
- Lack of impact assessments or consolidated risk management practices
- Missing cyber and/or legal subject matter expertise and technical support

- 66% of the reviewed entities are in noncompliance with Utah Code § 63D-2-103, the requirement to publish a Privacy Policy Statement on their websites.

Recommendations

We recommend:

- The SPO to continue to continue to support designated government entities, focusing on high-risk entities and their record retention practices.
- The SPO to expand their efforts on providing entities with templates of notices and policies to implement.
- The SPO to assist entities in designing monitoring controls to mitigate privacy risk.
- The State Legislature to provide additional funding allowing the SPO team to grow and have greater reach and guide entities toward faster improvement of the privacy landscape.
- The State Legislators to continue to improve legislative clarity and allow for more comprehensive legal mechanisms to be entered into the current Utah Code to achieve higher levels of data protection. The SPO has presented specific suggestions to the Personal Privacy Oversight Commission (PPOC).
- The designated government entities to allocate appropriate resources, enabling them to address non-compliance with existing legal requirements and allow for the implementation of the recommended monitoring metric and maturing their programs.

Annual Report Details

FY 2023 State Privacy Officer Achievements

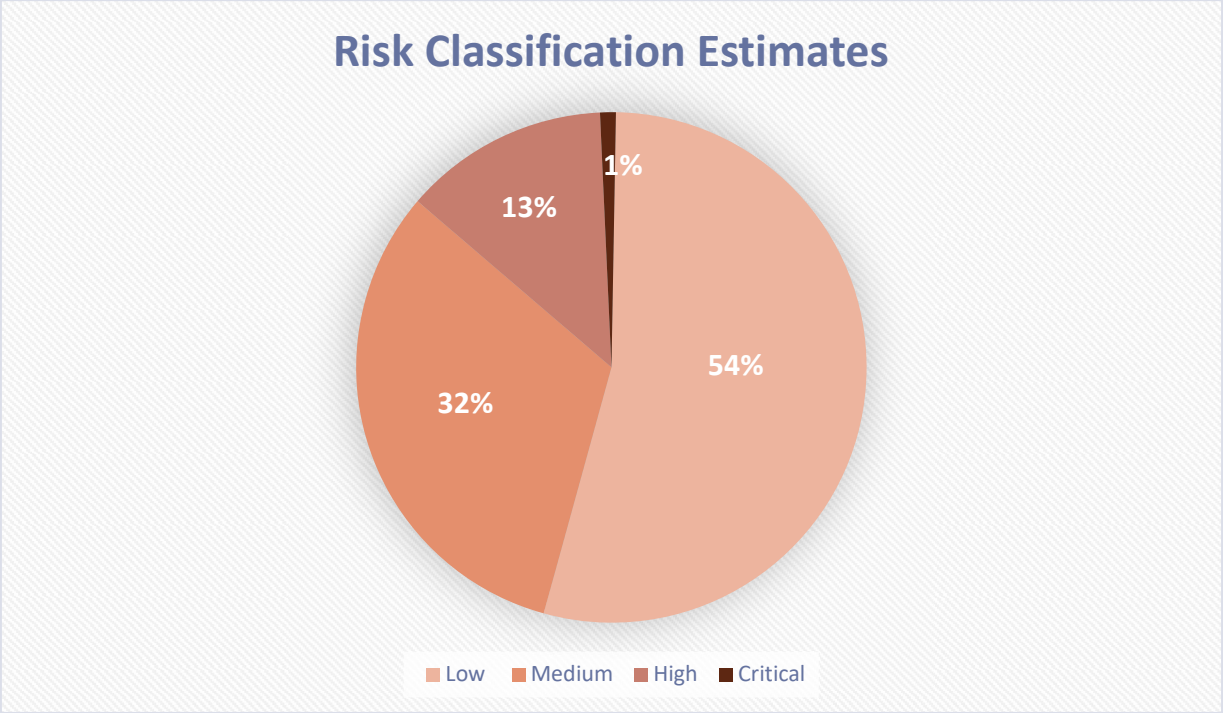
The SPO has completed the following achievements:

- Created a Privacy Plan to outline main goals for the year, metrics to monitor achievement of such goals, and to measure maturity assessments of the monitored privacy environment.
- Created an Impact Assessment Tool and piloted it with selected entities.
- Conducted 5 reviews.
- Reviewed 35 bills during the legislative sessions and provided feedback and recommendations to legislators.
- Conducted 30 individual training sessions with target audiences from education, law enforcement, counties, towns and cities. Sessions spanned from small, in-person groups to large, online groups. These sessions included state as well as national participants. Training reached an overall audience of over 8,000 unique participants.
- Created and disseminated various training materials focusing on: data privacy basics, incident response, breach notification obligations, working with AI within law enforcement, FERPA applications, and privacy contractual clauses.
- Drafted an outline of the new government privacy act that would improve the privacy landscape and introduced it to the PPOC.
- Measured compliance with Utah Code § 63D-2-103 which requires having a Privacy Statement Notice on websites of government entities that may process personal information.

Risk Classification

The SPO has created a risk assessment formula to analyze the risk level per entity and using an internally developed script applied this formula upon 1,600+ entities, to evaluate and sort them by risk into several categories.

Figure 1. Each entity had estimated risk classification assigned.



Each entity can be classified as belonging into one of the four following categories:

- Critical: 1% of entities
- High: 13% of entities
- Medium: 32% of entities
- Low: 54% of entities

The determination of risk level is based on the following factors:

1. Likelihood of processing sensitive data (student data, health care data, criminal records, etc.),
2. Size of the entity measured in employee count, and
3. Estimated number of constituents or population the entity serves.

Entities that serve the biggest population size and at the same time process sensitive data as part of their core operations, including large school districts and public safety entities, present the highest risk and thus are the primary focus of the SPO review.

Compliance

The SPO engaged a vendor to evaluate compliance of 1,617 designated government entities with Utah Code § 63D-2-103, which stipulates the requirement to have a Privacy Statement Notice on government entities' websites.

The code requires that the Privacy Statement Notice includes:

- The identity of the governmental website operator,
- Contact details for the governmental website operator,
- Overview of the personally identifiable information (PII) collected by the entity,
- Summary of how the PII is used by the entity,
- The practices related to disclosure of PII,
- The process to request access to or correction of the PII,
- Description of security measures applied to the PII.

The results of the check of compliance with this section of code are as follows:

Only 34% of reviewed entities published some form of a "Privacy Policy Statement" on their website, pertaining to collection of personal information from such websites' users.

Data Retention Period Disclosures: Although 11% of governmental websites have a privacy policy statement that includes a "data retention" disclosure, it is extremely rare for such data retention disclosure to present any specific retention periods

Academic Website Deficiencies: Websites for academic institutions often contain privacy-related notices, but such notices are often unrelated to collection of personal information from the websites' users and focus on FERPA.

Trainings and Awareness

As required by Utah Code § 67-3-13, the SPO raised awareness of legal obligations and conducted or participated in 30 educational sessions and trainings. For a full list see Appendix C.

Privacy Reviews

The SPO has met with selected entities across different risk levels to determine the overall privacy health of Utah designated government entities and establish a common baseline, assessing implementation and functionality of administrative, technical, and physical safeguards.

After assessing designated government entities across several risk categories, it was determined that while each of these entities processed regulated data in different quantities, they all exhibited similar gaps, mainly consisting in a lack of:

- Codified policies,
- Data inventories,
- Systemic reviews and monitoring of compliance,
- Dedicated privacy functions, and

- Consistent cyber security reviews and/or expertise.

While many entities employed good practices, it was only sporadically that the Utah Fundamental Privacy Principles (see Appendix D) were implemented and documented across any given entity.

All reviewed entities fall under the "ad-hoc" maturity level, pertaining to their privacy practices. Ad-hoc maturity level consists of some practices and policies in place, but without being codified or consolidated in a comprehensible, repeatable, and measurable program. Privacy functions are either missing or not embedded into the designated government entity. Privacy is not considered a core value. For additional levels see Appendix E.

The next step up to privacy maturity is "repeatable," with 12 months as a realistic goal to achieve an advanced level for all reviewed entities, under the guidance of the SPO.

Additional Assistance Provided

- The SPO developed a Privacy Impact Assessment Tool and piloted it on several projects, assisting designated government entities assess and mitigate privacy risk.
- The SPO regularly responded to requests for expertise throughout 2023, such requests were mostly related to the processing of mental / health records and assisting with risk mitigation in contractual documents.
- The SPO revised the process to accept and respond to complaints and has addressed multiple complaints throughout 2023.

2023 Legislative Review

As required by Utah Code § 67-3-13, the office conducted a review of the current privacy landscape in Utah affecting the designated government entities and provided recommendations during the legislative session (for a detailed list of reviewed bills see Appendix F).

The 2023 Legislative Session Key Recommendations Made

The SPO recommended substantial changes to;

- **HB 311 and SB 152**: Upholding Utah resident's privacy rights as related to the obligation to provide personal information to a Social Network Media or a third party engaged in conducting age verification on behalf of the Social Network Media, as required by HB 152.
- **HB 303**: The SPO recommended not linking victims of domestic violence to a special status as it could identify an already vulnerable individual based on whether the status of their voting records is hidden or public. Furthermore, the SPO recommended offering greater privacy protection to all Utah voters by limiting the groups that have access to voter's records

- **HB 57**: The SPO recommended keeping the requirement to access geolocation and other personal data related to drivers only based on a warrant

Additional recommendations were made to legislators related to limiting collection, access and dissemination of data, as well as adjusting definitions to create a more coherent environment.

2024 Goals

- The SPO will provide the recommended monitoring metrics (Appendix G) to all entities, with focus on high and critical risk entities to voluntarily collect and measure these as a best risk mitigating practice and will support their implementation.
- The SPO will continue to work with legislators and the PPOC to improve the privacy landscape for the designated government entities and introduce more clarity and unification across the Code.
- The SPO will continue to focus on offering regular training opportunities.
- The SPO will focus on reviews of entities within the "Critical" level of risk assessment.
- The SPO will expand the use of the Privacy Impact Assessments.

Certified Records Officers (R.O.) Metrics

Table 1. Summary of entities with a listed Records Officer by entity category, sorted by rate of compliance.

Entity Category	Number of Entities	Number of RO and %	
Public School	217	214	= 98.62%
County	243	238	= 97.94%
State Agency	749	699	= 93.32%
Municipality	499	441	= 88.38%
Associations of Government	8	7	= 87.50%
Charter School	142	122	= 85.92%
Special Service District	527	425	= 80.65%
Interlocal	24	18	= 75.00%
College or University	40	26	= 65.00%
Independent or Quasi-Government	19	9	= 47.37%
Other	20	8	= 40.00%
Local District	27	4	= 14.81%

Table 2. Summary of entities with active Records Officer certifications by entity category sorted by rate of compliance.

Entity Category	Number of Entities	Certified RO	Listed and %
State Agency	749	652	= 87.05%
Interlocal	24	19	= 79.17%
Municipality	499	377	= 75.55%
County	243	180	= 74.07%
Charter School	142	101	= 71.13%
Special Service District	527	339	= 64.33%
Public School	217	138	= 63.59%
Associations of Government	8	5	= 62.50%
College or University	40	24	= 60.00%
Other	20	10	= 50.00%
Independent or Quasi-Government	19	7	= 36.84%
Local District	27	3	= 11.11%

Metrics from Education

The education general compliance metric captures improvement between FY2022 and FY2023.

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

Yearly trend of compliance:

FY2022: 51%

FY2023: 68%

Metadata dictionary compliance: Utah Code § 53E-9-303 requires districts and charter schools to create a "metadata dictionary." According to Utah Code § 53E-9-301, the metadata dictionary is a record that defines and discloses all student PII that is collected and shared by the education entity; provides lists of all recipients with whom the education entity has shared the data; provides purpose, justification and legal basis for such disclosure; and is displayed on the education entity's website without disclosing the PII itself.

FY2022: 5%

FY2023: 54%

For an overview of the local education agency privacy compliance requirements see Appendix H.

Appendix A. Entity Overview

As of September 2023, the in-scope designated government entities include:

- 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

Appendix B. Authorities of the Utah Privacy Program

- Division of Archives and Records Services
  Utah Code § 63A-12-100 et seq. (AKA Public Records Management Act (PRMA))
- 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
- Personal Privacy Oversight Commission
  Utah Code § 63C-24-101 et seq.
- SPO (Auditor)
  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
  UT-ADC 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

Upcoming

- Student Data Privacy Training: St. George – FERPA for Higher Education- November 9, 2023
- Student Data Privacy Training: Springville – FERPA for Higher Education- November 8, 2023
- Student Data Privacy Training: Ogden – FERPA for Higher Education – November 7, 2023
- University of Utah – Privacy Coordination for Higher Education – November 7, 2023
- Government Cyber Insights – Utah's Focus on Privacy – October 29, 2023
- SAINTCON – Privacy Policies for Government Entities – October 26, 2023
- UCTL Webinar – Privacy Policies for Government Entities – October 18, 2023

Conducted

- Airport Law Enforcement Agencies Network- AI Privacy for Airports – September 26, 2023
- Utah's New Data Breach Reporting Requirements – September 13, 2023
- Presentation to Personal Privacy Oversight Commission – August 23, 2023
- Utah Rural School Association – Minimizing Digital Footprint – July 13 2023
- International Association of Chiefs of Police Technology Leadership – Privacy in Law Enforcement – June 21, 2023
- Privacy in Higher Education – FERPA for Higher Education: Utah State – June 8, 2023
- Utah Association of Counties Conference – 2023 Legislation Privacy Updates, April 27, 2023
- Update to Personal Privacy Oversight Commission – April 5, 2023
- ARMA – Conference Privacy Considerations for Records Management – March 16, 2023
- Brigham Young University Adam Smith Society – Privacy and Social Media Bills – March 15, 2023
- TCC – Privacy Health Checks – March 13, 2023
- Politico – Privacy: Who's Winning (video event) – March 1, 2023
- ABA Anti-Trust Law Section Membership Committee – The Importance of Mentorship – February 22, 2023
- Update to Personal Privacy Oversight Commission – February 8,2023
- Future of Wireless Retreat – Privacy Updates – January 17, 2023
- Presentation to Personal Privacy Oversight Commission – SPO Annual Report Summary – December 7, 2022

- Utah Association of Counties (UAC) Conference – Privacy Policies – November 16, 2022
- Utah Community Research Ethics Conference 2022 – The Future of Privacy in Utah: A Conversation with Utah's Privacy Officer – November 9, 2022
- Utah League of Cities and Towns Webinar – Privacy Basics- Don't say the "B" word! – October 18, 2022
- TCC – Privacy Updates – October 5, 2023
- SPO Annual Report FY2022 – October 1, 2022
- Presentation by SPO to Personal Privacy Oversight Commission – July 6, 2022

Appendix D. Utah Fundamental Privacy Principles

1. **Individual Participation**
   Give people control of their information when possible.
2. **Lawful, Fair, and Responsible use**
   Collection, use and disclosure is:
   - Based on legal authority;
   - Not deceptive
   - Not discriminatory or harmful; and
   - Relevant and readably necessary for legitimate purposes.
3. **Data Minimization**
   The minimum amount of information is collected, used, or disclosed to accomplish the stated purpose for collecting the information.
4. **Transparency and Accountability**
   Transparency means being open and transparent about what personal information is collected, for what purposes, and who it is shared with under what circumstances.
   Accountability means being responsible and answerable for following data privacy laws and principles.
5. **Security**
   Appropriate administrative, technical and physical security practices to protect the confidentiality, integrity, availability and control of personal information.
6. **Due Diligence**
   Taking reasonable steps and exercising care before and after entering into an agreement or arrangement with a third party that includes sharing personal information.

Appendix E. 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 policies on privacy exist.

Ad-Hoc

Privacy officer/privacy management function responsibilities exists and the role is known throughout the agency. Privacy 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 F. 2023 Legislative Review

Reviewed and Passed Legislation

- H.B. 457 State Property Transfer Amendments
- S.B. 227 Consumer Privacy Act
- H.B. 57 Law Enforcement Investigation Amendments
- S.B. 168 State Agency Capital Development Fund
- H.B. 18 Online Dating Safety Amendments
- H.B. 19 Rape Crisis Center Modifications
- H.B. 23 Forensic Mental Health Amendments
- S.B. 152 Social Media Regulation Amendments
- H.B. 311 Social Media Usage Amendments
- H.B. 303 Elections Record Amendments
- H.B. 470 Government Digital Verifiable Record Amendments
- S.B. 124 Law Enforcement Officer Amendments
- S.B. 156 Investigative Genetic Genealogy Modifications
- H.B. 61 School Safety Requirements
- H.B. 304 Juvenile Justice Revisions
- H.B. 312 Patient Medical Record Access Amendments
- H.B. 343 Government Records Modifications
- H.B. 352 Law Enforcement Data Amendments
- H.B. 368 Inmate Identification Amendments
- S.B. 41 Health and Human Services Recodification - Prevention, Supports, Substance Use and Mental Health
- S.B. 100 School Gender Identity Policies
- S.B. 127 Cybersecurity Amendments

Reviewed Legislation That Did Not Pass

- H.B. 242 Services for People with Disabilities Amendments
- H.B. 459 Governmental Immunity Amendments
- H.B. 457 Consumer Data Privacy Amendments
- H.B. 60 Juvenile Record Modifications
- H.B. 158 Electronic Information or Data Privacy Act Modifications

- H.B. 29 Mental Health Support and Law Enforcement Co-response
- H.B. 168 License Plate Reader Systems Amendments
- H.B. 81 Mental Health Treatment Amendments
- H.B. 404 Juvenile Interrogation Modifications
- H.B. 483 Health Evaluations for Driving Amendments
- H.B. 516 Mental Health Treatment Study
- H.B. 529 Food Shopping History Requirements
- S.B. 105 Traffic Enforcement

Appendix G. Monitoring Recommendations, Individual Metrics

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 non-compliance 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 H. Local Education Agency Privacy Compliance 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 1232h(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 are 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