

PRIVACY PROGRAM REPORT TEMPLATE

Disclaimer: This template is provided by the Utah Office of Data Privacy (ODP) as a resource to assist governmental entities. **This template is intended to serve as general guidance and a foundational structure only.** Governmental entities are responsible for reviewing, customizing, and adapting this template to ensure compliance with applicable laws, regulations, policies, and organizational needs.

The ODP makes no representations or warranties, express or implied, regarding the legal sufficiency or suitability of this template for any specific purpose. By using this template, governmental entities acknowledge and agree that the ODP is not liable for the use or modification of this template. **This template is not legal advice and is not a substitute for consultation with legal counsel.** Entities should consult with their own legal counsel before finalizing or executing a document based on this template.

Version History located in Appendix A.



UTAH OFFICE *of*
DATA PRIVACY

4315 S 2700 W, Taylorsville, UT 84129

officeofdataprivacy@utah.gov | privacy.utah.gov

Privacy Program Report Template v1.1

Each governmental entity must complete a Privacy Program Report (Report) before December 31st of each year. The Report must be prepared and certified by the chief administrative officer (CAO) of the governmental entity. Completion of the Report satisfies the requirement that the governmental entity initiate a data privacy program as required by Utah Code § 63A-19-401(2)(a)(i). The Report is a protected record under Utah Code § 63G-2-305 but may be provided to the Office upon request.

Definitions: Terms used in this Report are defined in Utah Code § 63A-19-101.

SECTION 1: GOVERNMENTAL ENTITY INFORMATION

Name: _____

Type (Select One):

State Agency

County

Municipality

Special Service District

Board or Commission

College or University

Other _____

Interlocal

Associations of Government

Charter School

Special District

Independent or Quasi-Government

Public School

Mailing Address: _____

Chief Administrative Officer (CAO):

Name: _____

Title: _____

Email: _____

Phone: _____

SECTION 2: PRIVACY PROGRAM STATUS

The Report must include whether the governmental entity has initiated a privacy program. (Utah Code § 63A-19-401.3(1)(a)) A privacy program is the structured collection of a governmental entity's privacy practices, policies, and procedures that govern its processing and protection of personal data to ensure compliance with applicable laws. A governmental entity's privacy program will meet the December 31, 2025, deadline even if it is not mature or if it is in its early stages, so long as the entity has fully completed its privacy program report or initiated its program through other means that the entity has determined as meeting the requirements of the Government Data Privacy Act (GDPA).

Has your governmental entity initiated a privacy program?

Yes

No

How has the governmental entity initiated a privacy program?

Administrative Rule

Ordinance

Resolution

Policy

Privacy Program Report

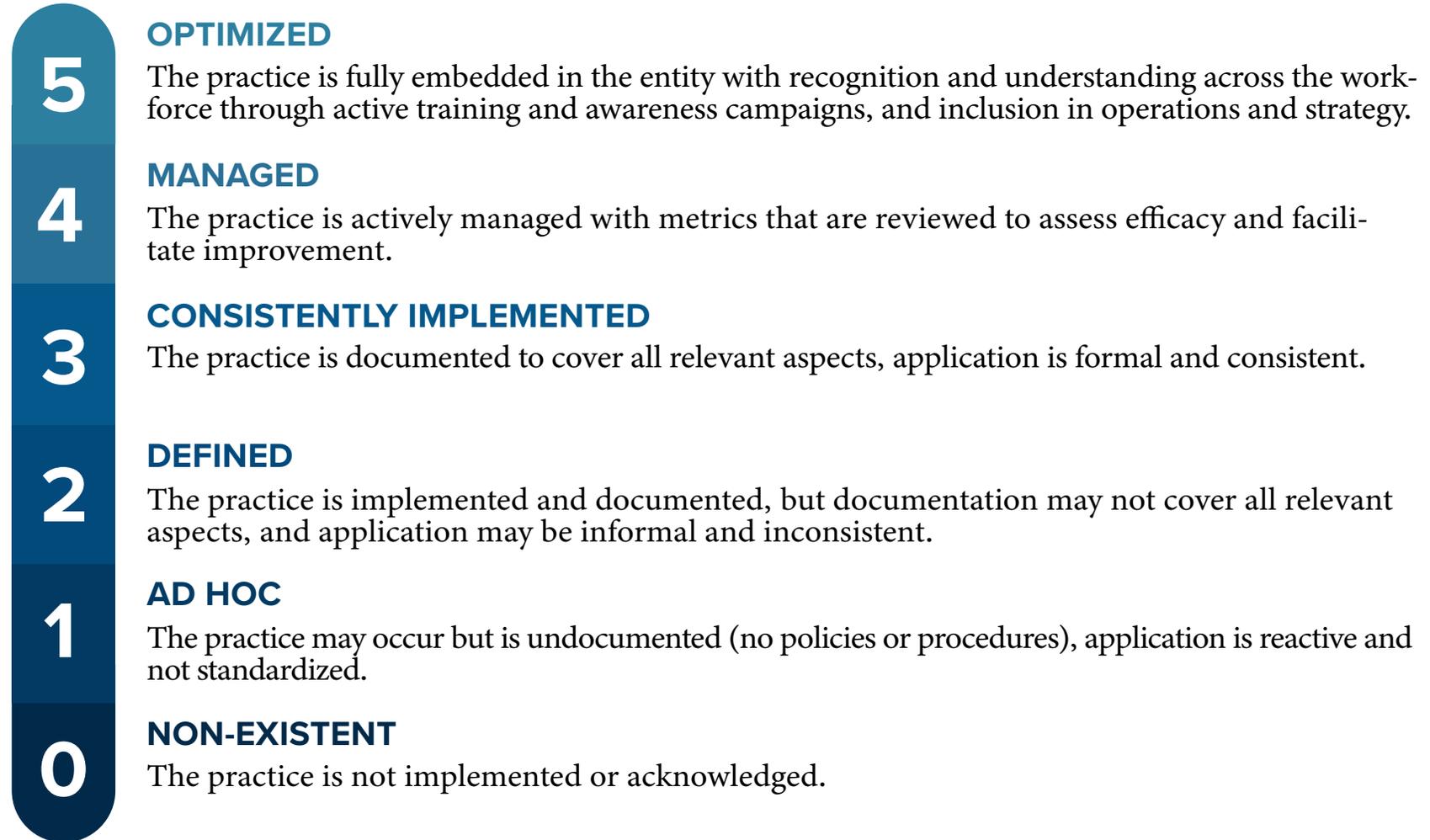
Other _____

SECTION 3: PRIVACY PRACTICES, MATURITY AND STRATEGIES

The Report must include any privacy practices implemented by the governmental entity and strategies for improving the governmental entity's privacy program and practices. (Utah Code § 63A-19-401.3(1)(b)(i) and (ii)). The privacy practices listed below are discussed in the Privacy Program Framework (Framework), which the Office created and maintains, and which may be accessed on privacy.utah.gov. The Framework includes privacy practice requirements that are generally required by governmental entities as established in the GDPA, Title 63G, Chapter 2, Government Records Access and Management Act (GRAMA), Title 63A, Chapter 12, Division of Archives and Records Service and Management of Government Records (DARSMGR), and some administrative rules. The Framework also includes a maturity model that entities may use to internally assess the maturity of a specific practice and create strategies to mature a specific practice.

Although using the maturity matrix is not required at this time, the Office recommends that entities use the maturity matrix in conjunction with the Framework and other assistance the Office provides. Any other applicable privacy practices required by sector specific laws or regulations should also be included.

PRIVACY MATURITY MODEL



PRIVACY PRACTICES IMPLEMENTED:

Check all privacy practices the governmental entity has implemented so far, and describe the strategies the governmental entity will use in the coming calendar year to improve its privacy practices and program. The Office recommends entities indicate the current maturity level (0–5) of each practice and select the target maturity they plan to achieve for a given practice by the end of the following calendar year. This will be beneficial to the governmental entity in moving their privacy programs forward.

 GOVERN				
PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
1.1 Chief Administrative Officer (CAO) Designation	Yes No			
1.2 Records Officers Appointment	Yes No			

1.3 Records Officer Training and Certification	Yes No			
1.4 Statewide Privacy Training	Yes No			
1.5 Privacy Program Report	Yes No			

IDENTIFY

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
2.1 Record Series Creation and Maintenance	Yes No			
2.2 Record Series Designation and Classification	Yes No			
2.3 Statement Filed with State Archivist	Yes No			

2.4 Retention Schedule Proposal and Approval	Yes No			
2.5 Record Series Privacy Annotation	Yes No			
2.6 Inventorying	Yes No			
2.7 Privacy Impact Assessments (PIA)	Yes No			

2.8 Record and Data Sharing, Selling, or Purchasing	Yes No			
---	-----------	--	--	--

CONTROL

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
3.1 Data Subject Requests for Access	Yes No			
3.2 Data Subject Requests for Amendment or Correction	Yes No			

3.3 Data Subject Requests for an Explanation	Yes No			
3.4 Data Subject Request by At-Risk Employees for Restricting Access	Yes No			

COMMUNICATE

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
4.1 Privacy Notice (Notice to Provider of Information)	Yes No			

4.2 Website Privacy Notice and Website Privacy Policy	Yes No			
---	-----------	--	--	--

PROTECT

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
5.1 Minimum Data Necessary	Yes No			
5.2 Retention and Disposition of Records Containing Personal Data	Yes No			

5.3 Incident Response and Notification to the Cyber Center and Attorney General	Yes No			
5.4 Breach Notification to Affected Individuals	Yes No			

OTHER PRIVACY PRACTICES IMPLEMENTED BY THE GOVERNMENTAL ENTITY

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
	Yes No			

	Yes No			
	Yes No			

SECTION 4: SHARING, SELLING, AND PURCHASING PERSONAL DATA

The Report must include a list of the types of personal data the governmental entity currently shares, sells, or purchases; the legal basis for sharing, selling, or purchasing personal data; and the category of individuals or entities with whom the governmental entity shares personal data, to whom the governmental entity sells personal data, and from whom the governmental entity purchases personal data. (Utah Code § 63A-19-401.3(1)(c), (d), and (e))

Using the check boxes below identify whether, and the types of, personal data the governmental entity shares, sells, or purchases and provide a summary of the legal basis for the sharing, selling, or purchasing.

TYPES OF PERSONAL DATA	SHARE, SELL, AND PURCHASE STATUS	LEGAL BASIS FOR SHARING, SELLING, AND PURCHASING
<p>Basic Identification & Contact Information</p> <ul style="list-style-type: none"> • Full Name • Date of Birth • Place of Birth • Gender • Age • Government-Issued Identifiers: <ul style="list-style-type: none"> • Social Security Number • Driver's License or State ID Number • Passport Number • Other national or government-assigned IDs • Contact Information: <ul style="list-style-type: none"> • Home Address • Email Address(es) • Phone Number(s) • Mailing Address (if different from home address) 	<p>Share Sell Purchase N/A</p>	
<p>Demographic & Personal Characteristics</p> <ul style="list-style-type: none"> • Race or Ethnicity • Marital Status • Nationality or Citizenship • Language Preferences • Household Information <ul style="list-style-type: none"> • Household Size • Household Composition 	<p>Share Sell Purchase N/A</p>	

<p>Employment & Professional Information</p> <ul style="list-style-type: none"> • Job Title and Position • Employment History • Employer Name • Professional Credentials <ul style="list-style-type: none"> • Professional Licenses • Certifications • Work Contact Information 	<p>Share Sell Purchase N/A</p>	
<p>Financial Data</p> <ul style="list-style-type: none"> • Banking Details <ul style="list-style-type: none"> • Bank Account Numbers • Credit Card Numbers • Tax Identification Numbers • Income and Wage Data • Credit Information <ul style="list-style-type: none"> • Credit Reports • Credit Scores • Payment History 	<p>Share Sell Purchase N/A</p>	
<p>Health and Medical Information</p> <ul style="list-style-type: none"> • Medical History • Diagnoses or Treatments • Mental Health Data • Health Insurance Information • Prescription Information • Disability Status 	<p>Share Sell Purchase N/A</p>	

<p>Education Information</p> <ul style="list-style-type: none"> • School or Institution Attended • Student ID Numbers • Academic Records <ul style="list-style-type: none"> • Grades • Transcripts • Special Education Status • Disciplinary Records 	<p>Share Sell Purchase N/A</p>	
<p>Government Program & Benefits Data</p> <ul style="list-style-type: none"> • Program Participation (e.g., SNAP, Medicaid, TANF) • Eligibility Determinations • Benefit Amounts or Disbursements • Case Management Notes • Appeals/Decisions 	<p>Share Sell Purchase N/A</p>	
<p>Biometric Data</p> <ul style="list-style-type: none"> • Physical Biometrics <ul style="list-style-type: none"> • Fingerprints • Facial Recognition Data • Retina or Iris Scans • Voiceprints • Genetic Information: DNA or other genetic data 	<p>Share Sell Purchase N/A</p>	

<p>Online & Digital Identifiers</p> <ul style="list-style-type: none"> • Network Identifiers • IP Addresses • Device IDs • Tracking Technologies • Cookies • Browser Fingerprints • Location Data (e.g., GPS, precise geolocation) • Login Credentials (e.g., usernames, hashed passwords) • Online Activity Logs • Social Media Handles 	<p>Share Sell Purchase N/A</p>	
<p>Criminal or Legal Information</p> <ul style="list-style-type: none"> • Arrest Records • Conviction History • Court Records • Probation or Parole Status • Incarceration Records 	<p>Share Sell Purchase N/A</p>	
<p>Vehicle & Property Data</p> <ul style="list-style-type: none"> • Vehicle Information • Vehicle Registration • VIN Numbers • Property Ownership • Property Ownership or Deed Information • Property Tax Records • Utility Usage Data 	<p>Share Sell Purchase N/A</p>	

<p>Photographic or Video Data</p> <ul style="list-style-type: none"> • Surveillance Footage • Government ID Photos • School or Agency-Provided Photo Records • Body Camera Footage • Public Meeting Recordings 	<p>Share Sell Purchase N/A</p>	
<p>Voting & Civic Data</p> <ul style="list-style-type: none"> • Voter Registration • Voting History • Political District Assignments • Civic Engagement Program Data 	<p>Share Sell Purchase N/A</p>	
<p>Immigration & Travel Information</p> <ul style="list-style-type: none"> • Visa Status • Travel History or Itineraries • Customs Declarations • Immigration Proceedings 	<p>Share Sell Purchase N/A</p>	
<p>Communication & Complaints Data</p> <ul style="list-style-type: none"> • Correspondence <ul style="list-style-type: none"> • Emails or Written Correspondence • Call Transcripts or Recordings • Case Notes related to complaints or service requests 	<p>Share Sell Purchase N/A</p>	

Other:	Share Sell Purchase N/A	
Other:	Share Sell Purchase N/A	
Other:	Share Sell Purchase N/A	

SECTION 5: PERSONAL DATA RECIPIENTS AND SOURCES

Fulfills requirements of Subsections 63A-19-401.3(1)(e)(i), (ii), and (iii):

Mark any categories of individuals or entities with whom personal data is shared, to whom personal data is sold, and from whom personal data is purchased.

PROCESSING ACTIVITY	CATEGORIES OF RECIPIENTS OR SOURCES
<p>Personal Data Shared With:</p>	<p>Governmental and Public Sector Entities</p> <ul style="list-style-type: none"> I. Domestic Governmental Entities: <ul style="list-style-type: none"> State, Local, Federal, or Tribal Governmental Entities Law Enforcement Agencies Judicial or Court Systems Legislative Bodies or Policy Research Organizations Regulatory Agencies Professional Licensing Boards II. International Governmental Entities: <ul style="list-style-type: none"> Foreign Governments or International Organizations Public Services & Emergency: <ul style="list-style-type: none"> Emergency Services / Disaster Response Agencies Public Utilities or Infrastructure Partners III. Public Disclosure: <ul style="list-style-type: none"> Public Disclosure / Open Records Releases <p>Commercial and Private Sector Entities</p> <ul style="list-style-type: none"> I. Service Providers & Vendors: <ul style="list-style-type: none"> Third-Party Service Providers / Contractors / Vendors Cloud Service Providers / Hosting Platforms Technology Integrators or Software Developers II. Data & Marketing: <ul style="list-style-type: none"> Private Sector / Commercial Companies Data Brokers / Aggregators Social Media Platforms III. Financial & Insurance: <ul style="list-style-type: none"> Credit Bureaus or Financial Institutions Insurance Providers IV. Healthcare: <ul style="list-style-type: none"> Healthcare Providers or Health Information Exchanges V. Media: <ul style="list-style-type: none"> Media or News Organizations <p>Research, Education, and Nonprofit Entities</p> <ul style="list-style-type: none"> Research Institutions / Universities

<p>Personal Data Sold To:</p>	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities: State, Local, Federal, or Tribal Governmental Entities Law Enforcement Agencies Judicial or Court Systems Legislative Bodies or Policy Research Organizations Regulatory Agencies Professional Licensing Boards</p> <p>II. International Governmental Entities: Foreign Governments or International Organizations Public Services & Emergency: Emergency Services / Disaster Response Agencies Public Utilities or Infrastructure Partners</p> <p>III. Public Disclosure: Public Disclosure / Open Records Releases</p> <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors: Third-Party Service Providers / Contractors / Vendors Cloud Service Providers / Hosting Platforms Technology Integrators or Software Developers</p> <p>II. Data & Marketing: Private Sector / Commercial Companies Data Brokers / Aggregators Social Media Platforms</p> <p>III. Financial & Insurance: Credit Bureaus or Financial Institutions Insurance Providers</p> <p>IV. Healthcare: Healthcare Providers or Health Information Exchanges</p> <p>V. Media: Media or News Organizations</p> <p>Research, Education, and Nonprofit Entities Research Institutions / Universities</p>
-------------------------------	---

<p>Personal Data Purchased From:</p>	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities: State, Local, Federal, or Tribal Governmental Entities Law Enforcement Agencies Judicial or Court Systems Legislative Bodies or Policy Research Organizations Regulatory Agencies Professional Licensing Boards</p> <p>II. International Governmental Entities: Foreign Governments or International Organizations Public Services & Emergency: Emergency Services / Disaster Response Agencies Public Utilities or Infrastructure Partners</p> <p>III. Public Disclosure: Public Disclosure / Open Records Releases</p> <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors: Third-Party Service Providers / Contractors / Vendors Cloud Service Providers / Hosting Platforms Technology Integrators or Software Developers</p> <p>II. Data & Marketing: Private Sector / Commercial Companies Data Brokers / Aggregators Social Media Platforms</p> <p>III. Financial & Insurance: Credit Bureaus or Financial Institutions Insurance Providers</p> <p>IV. Healthcare: Healthcare Providers or Health Information Exchanges</p> <p>V. Media: Media or News Organizations</p> <p>Research, Education, and Nonprofit Entities Research Institutions / Universities</p>
--------------------------------------	---

SECTION 6: NON-COMPLIANT PROCESSING ACTIVITIES

The Report must include a description of any non-compliant processing activities identified under Subsection [63A-19-401\(2\)\(a\)\(iv\)](#) and the governmental entity's strategy for bringing those activities into compliance with the GDPR. (Utah Code § 63A-19-401.3(1)(g))

PROCESSING ACTIVITY	STRATEGIES FOR COMPLIANCE

SECTION 7: HIGH-RISK PROCESSING ACTIVITIES

The Report must include a description of the governmental entity's high-risk processing activities. (Utah Code § 63A-19-401.3(1)(b)(iii))

Select all applicable high-risk processing activities the entity engages in and explain why the governmental entity engages in the high-risk processing activity.

Facial recognition technology

Description of Purpose: _____

Automated decision making

Description of Purpose: _____

Profiling (e.g., behavioral or predictive analysis)

Description of Purpose: _____

Genetic data processing

Description of Purpose: _____

Biometric data processing (e.g., fingerprints, voice, iris scans)

Description of Purpose: _____

Geolocation data processing

Description of Purpose: _____

List any other processing activities the entity has identified as high-risk under the statutory definition and a brief description of the purposes and uses of each.

SECTION 8: PRIVACY TRAINING COMPLETION

The Report must include the percentage of the governmental entity's employees that have fulfilled the data privacy training requirements described in Utah Code § 63A-19-401.2. (Utah Code § 63A-19-401.3(1)(f))

What percentage of the entity's employees have completed the required data privacy training created by the Office?

Enter %

SECTION 9: CERTIFICATION

I hereby certify that I am the Chief Administrative Officer for the governmental entity named above, and the information provided in this report is accurate to the best of my knowledge.

Name: _____

Signature: _____

Date: _____

APPENDIX A

VERSION HISTORY

Version 1.0 - Original Version.

Version 1.1 - Updated design, definitions and questions simplified, sections rearranged, Special District added to list of entity types