VERSION 1.1

PRIVACY PROGRAM REPORT TEMPLATE

Utah Office *of* Data Privacy

SAMPLE — fictional data

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.

SAMPLE — fictional data — DRAFT for review

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.

The report must be shared with the office, in accordance with Section 63G-2-206, on or before December 31 of each year; and retained by the governmental entity for no less than five years.

Instructions: Email the completed report to officeofdataprivacy@utah.gov.

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

Version History located in Appendix A.

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

SECTION 1: GOVERNMENTAL ENTITY INFORMATION

Name: Juniper Hollow Special Service District (Sample — fictional)

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: 43 Sample Cloudberry Spur, Sample Pinecrest County, UT 00000 (fictional)

Chief Administrative Officer (CAO):

Name: Mira Sample Quill (fictional)

Title: Sample District Administrator

Email: mira.sample@example.org

Phone: 801-555-0142

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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 _____

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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.

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

PRIVACY MATURITY MODEL



OPTIMIZED

The practice is fully embedded in the entity with recognition and understanding across the workforce through active training and awareness campaigns, and inclusion in operations and strategy.

MANAGED

The practice is actively managed with metrics that are reviewed to assess efficacy and facilitate improvement.

CONSISTENTLY IMPLEMENTED

The practice is documented to cover all relevant aspects, application is formal and consistent.

DEFINED

The practice is implemented and documented, but documentation may not cover all relevant aspects, and application may be informal and inconsistent.

AD HOC

The practice may occur but is undocumented (no policies or procedures), application is reactive and not standardized.

NON-EXISTENT

The practice is not implemented or acknowledged.

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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	Level 2	Sample: confirm CAO designation in the annual board review.	Level 3
1.2 Records Officers Appointment	☑ Yes ☐ No	Level 2	Sample: document the records officer backup and duties by March.	Level 3

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

1.3 Records Officer Training and Certification	☑ Yes ☐ No	Level 2	Sample: renew records-officer training and file the certificate.	Level 3
1.4 Statewide Privacy Training	☑ Yes ☐ No	Level 1	Sample: schedule the fourth employee and keep a completion log.	Level 2
1.5 Privacy Program Report	☑ Yes ☐ No	Level 1	Sample: complete CAO review and retain the approved annual report.	Level 2

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

IDENTIFY

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
2.1 Record Series Creation and Maintenance	☑ Yes ☐ No	Level 1	Sample: list billing, personnel, and meeting record series.	Level 2
2.2 Record Series Designation and Classification	☑ Yes ☐ No	Level 1	Sample: review series classifications with the records officer.	Level 2
2.3 Statement Filed with State Archivist	☑ Yes ☐ No	Level 1	Sample: verify and update the statement with the State Archivist.	Level 2

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

2.4 Retention Schedule Proposal and Approval	☑ Yes ☐ No	Level 2	Sample: confirm schedules cover all current record series.	Level 1
2.5 Record Series Privacy Annotation	☐ Yes ☑ No	Level 0	Sample: annotate personal data in billing and personnel series.	Level 1
2.6 Inventorying	☑ Yes ☐ No	Level 1	Sample: inventory paper files, shared drives, and vendor systems.	Level 2
2.7 Privacy Impact Assessments (PIA)	☐ Yes ☑ No	Level 0	Sample: adopt a short privacy-risk review before new software.	Level 1

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

2.8 Record and Data Sharing, Selling, or Purchasing	☐ Yes ☑ No	Level 2	Sample: record vendor disclosures and review access annually.	Level 2

CONTROL

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
3.1 Data Subject Requests for Access	☑ Yes ☐ No	Level 2	Sample: document intake, identity checks, deadlines, and escalation.	Level 3
3.2 Data Subject Requests for Amendment or Correction	☑ Yes ☐ No	Level 1	Sample: add correction requests to the records request log.	Level 2

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

3.3 Data Subject Requests for an Explanation	☑ Yes ☐ No	Level 1	Sample: publish a contact and response procedure for explanations.	Level 2
3.4 Data Subject Request by At-Risk Employees for Restricting Access	☑ Yes ☐ No	Level 1	Sample: prepare a restricted-access request checklist.	Level 2

COMMUNICATE

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
4.1 Privacy Notice (Notice to Provider of Information)	☑ Yes ☐ No	Level 1	Sample: add collection-purpose notices to the service application.	Level 2

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

4.2 Website Privacy Notice and Website Privacy Policy	☑ Yes ☐ No	Level 1	Sample: update the website policy after inventorying site logs.	Level 2

PROTECT

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
5.1 Minimum Data Necessary	☑ Yes ☐ No	Level 2	Sample: review intake forms and remove unnecessary identifiers.	Level 3
5.2 Retention and Disposition of Records Containing Personal Data	☑ Yes ☐ No	Level 1	Sample: log scheduled disposition and verify vendor deletion.	Level 2

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

5.3 Incident Response and Notification to the Cyber Center and Attorney General	☑ Yes ☐ No	Level 1	Sample: document incident contacts and run a tabletop exercise.	Level 2
5.4 Breach Notification to Affected Individuals	☑ Yes ☐ No	Level 1	Sample: prepare a notification checklist and review with counsel.	Level 2

OTHER PRIVACY PRACTICES IMPLEMENTED BY THE GOVERNMENTAL ENTITY

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
Sample quarterly access review	☑ Yes ☐ No	Level 1	Sample: review user accounts quarterly and remove stale access.	Level 2

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

Sample portable device safeguards	☑ Yes ☐ No	Level 1	Sample: inventory portable devices and verify encryption.	Level 2
Sample backup restore checks	☑ Yes ☐ No	Level 2	Sample: record a quarterly restore check for encrypted backups.	Level 3

SAMPLE — fictional data

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.

SAMPLE — fictional data — DRAFT for review

TYPES OF PERSONAL DATA	SHARE, SELL, AND PURCHASE STATUS	LEGAL BASIS FOR SHARING, SELLING, AND PURCHASING

Basic Identification & Contact Information
• Full Name
• Date of Birth
• Place of Birth
• Gender
• Age
• Government-Issued Identifiers:
  • Social Security Number
  • Driver's License or State ID Number
  • Passport Number
  • Other national or government-assigned IDs
• Contact Information:
  • Home Address
  • Email Address(es)
  • Phone Number(s)
  • Mailing Address (if different from home address)
	☑ Share
	☐ Sell
	☐ Purchase
	☐ N/A
		Sample: limited service-contact data goes to contracted billing and hosting processors for district operations. Public releases receive classification and redaction review under GRAMA (Utah Code Title 63G, Chapter 2). No sale or purchase.

Demographic & Personal Characteristics
• Race or Ethnicity
• Marital Status
• Nationality or Citizenship
• Language Preferences
• Household Information
  • Household Size
  • Household Composition
	☐ Share
	☐ Sell
	☐ Purchase
	☑ N/A	

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

Employment & Professional Information
• Job Title and Position
• Employment History
• Employer Name
• Professional Credentials
  • Professional Licenses
  • Certifications
• Work Contact Information
	☑ Share
	☐ Sell
	☐ Purchase
	☐ N/A	

Financial Data
• Banking Details
  • Bank Account Numbers
  • Credit Card Numbers
• Tax Identification Numbers
• Income and Wage Data
• Credit Information
  • Credit Reports
  • Credit Scores
• Payment History
	☑ Share
	☐ Sell
	☐ Purchase
	☐ N/A
		Sample: payment and payroll information goes to contracted payment processors and financial institutions for district operations. GRAMA classification and disclosure review apply; account details are withheld as appropriate. No sale or purchase.

Health and Medical Information • Medical History • Diagnoses or Treatments • Mental Health Data • Health Insurance Information • Prescription Information • Disability Status	☐ Share ☐ Sell ☐ Purchase ☑ N/A	

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

Education Information
• School or Institution Attended
• Student ID Numbers
• Academic Records
  • Grades
  • Transcripts
• Special Education Status
• Disciplinary Records
	☐ Share
	☐ Sell
	☐ Purchase
	☑ N/A	

Government Program & Benefits Data • Program Participation (e.g., SNAP, Medicaid, TANF) • Eligibility Determinations • Benefit Amounts or Disbursements • Case Management Notes • Appeals/Decisions	☐ Share ☐ Sell ☐ Purchase ☑ N/A	

Biometric Data
• Physical Biometrics
  • Fingerprints
  • Facial Recognition Data
  • Retina or Iris Scans
• Voiceprints
• Genetic Information: DNA or other genetic data
	☐ Share
	☐ Sell
	☐ Purchase
	☑ N/A	

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

Online & Digital Identifiers
• 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
	☐ Share
	☐ Sell
	☐ Purchase
	☑ N/A	

Criminal or Legal Information • Arrest Records • Conviction History • Court Records • Probation or Parole Status • Incarceration Records	☐ Share ☐ Sell ☐ Purchase ☑ N/A	

Vehicle & Property Data
• Vehicle Information
  • Vehicle Registration
  • VIN Numbers
• Property Ownership
  • Property Ownership or Deed Information
  • Property Tax Records
• Utility Usage Data
	☐ Share
	☐ Sell
	☐ Purchase
	☑ N/A	

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

Photographic or Video Data • Surveillance Footage • Government ID Photos • School or Agency-Provided Photo Records • Body Camera Footage • Public Meeting Recordings	☐ Share ☐ Sell ☐ Purchase ☑ N/A	
Voting & Civic Data • Voter Registration • Voting History • Political District Assignments • Civic Engagement Program Data	☐ Share ☐ Sell ☐ Purchase ☑ N/A	
Immigration & Travel Information • Visa Status • Travel History or Itineraries • Customs Declarations • Immigration Proceedings	☐ Share ☐ Sell ☐ Purchase ☑ N/A	

Communication & Complaints Data
• Correspondence
  • Emails or Written Correspondence
  • Call Transcripts or Recordings
• Case Notes related to complaints or service requests
	☑ Share
	☐ Sell
	☐ Purchase
	☐ N/A
		Sample: service correspondence may be released following GRAMA classification and redaction review. Contractors receive only the data needed to resolve service requests. No sale or purchase.

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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

SAMPLE — fictional data

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.

SAMPLE — fictional data — DRAFT for review

PROCESSING ACTIVITY	CATEGORIES OF RECIPIENTS OR SOURCES
Personal Data Shared With:	**Governmental and Public Sector Entities** 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 II. International Governmental Entities: ☐ Foreign Governments or International Organizations ☐ Public Services & Emergency: ☐ Emergency Services / Disaster Response Agencies ☐ Public Utilities or Infrastructure Partners III. Public Disclosure: ☑ Public Disclosure / Open Records Releases **Commercial and Private Sector Entities** I. Service Providers & Vendors: ☑ Third-Party Service Providers / Contractors / Vendors ☑ Cloud Service Providers / Hosting Platforms ☐ Technology Integrators or Software Developers II. Data & Marketing: ☐ Private Sector / Commercial Companies ☐ Data Brokers / Aggregators ☐ Social Media Platforms III. Financial & Insurance: ☑ Credit Bureaus or Financial Institutions ☐ Insurance Providers IV. Healthcare: ☐ Healthcare Providers or Health Information Exchanges V. Media: ☐ Media or News Organizations **Research, Education, and Nonprofit Entities** ☐ Research Institutions / Universities

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

Personal Data Sold To:	**Governmental and Public Sector Entities** 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 II. International Governmental Entities: ☐ Foreign Governments or International Organizations ☐ Public Services & Emergency: ☐ Emergency Services / Disaster Response Agencies ☐ Public Utilities or Infrastructure Partners III. Public Disclosure: ☐ Public Disclosure / Open Records Releases **Commercial and Private Sector Entities** I. Service Providers & Vendors: ☐ Third-Party Service Providers / Contractors / Vendors ☐ Cloud Service Providers / Hosting Platforms ☐ Technology Integrators or Software Developers II. Data & Marketing: ☐ Private Sector / Commercial Companies ☐ Data Brokers / Aggregators ☐ Social Media Platforms III. Financial & Insurance: ☐ Credit Bureaus or Financial Institutions ☐ Insurance Providers IV. Healthcare: ☐ Healthcare Providers or Health Information Exchanges V. Media: ☐ Media or News Organizations **Research, Education, and Nonprofit Entities** ☐ Research Institutions / Universities

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

Personal Data Purchased From:	**Governmental and Public Sector Entities** 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 II. International Governmental Entities: ☐ Foreign Governments or International Organizations ☐ Public Services & Emergency: ☐ Emergency Services / Disaster Response Agencies ☐ Public Utilities or Infrastructure Partners III. Public Disclosure: ☐ Public Disclosure / Open Records Releases **Commercial and Private Sector Entities** I. Service Providers & Vendors: ☐ Third-Party Service Providers / Contractors / Vendors ☐ Cloud Service Providers / Hosting Platforms ☐ Technology Integrators or Software Developers II. Data & Marketing: ☐ Private Sector / Commercial Companies ☐ Data Brokers / Aggregators ☐ Social Media Platforms III. Financial & Insurance: ☐ Credit Bureaus or Financial Institutions ☐ Insurance Providers IV. Healthcare: ☐ Healthcare Providers or Health Information Exchanges V. Media: ☐ Media or News Organizations **Research, Education, and Nonprofit Entities** ☐ Research Institutions / Universities

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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 GDPA. (Utah Code § 63A-19-401.3(1)(g))

PROCESSING ACTIVITY	STRATEGIES FOR COMPLIANCE
Sample: legacy service form lacks a collection notice.	Sample: CAO will add and review the notice by March 31, 2027.
Sample: billing records lack privacy annotations.	Sample: records officer will annotate the series by June 30, 2027.

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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.

Sample: no high-risk processing activities identified after staff review.

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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 who are required to complete data privacy training have completed data privacy training?

Enter % 75

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: Mira Sample Quill (fictional)

Sign here >

Signature: _____

Date: _____

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review

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

SAMPLE — fictional data

SAMPLE — fictional data — DRAFT for review