OFFICE OF THE
STATE AUDITOR

This document is for educational purposes only and needs to be customized further. Reach out to the State Privacy Officer at wphillips@utah.gov before implementation.

Personal Data Inventory Template

(this document is related to the Privacy Program requirement and the annual reporting requirement under The Utah Government Data Privacy Act)

Project /Purpose:

Describe the intended purpose of this data collection, group data by project:

Example:

Migrating a whole population of tenants into a new cloud environment to carry out HR services in a new tool that will allow for greater automation.

1. **Groups of individuals** affected by the data collection (check all that apply).

Employees	Tenants	Constituents	Minors	Customers
Contractors	3rd parties	Property owners	Students	Volunteers

Other groups (specify):

2. **Number of affected individuals:**
   1-100, 101-1000, 1001-10.000, 10.001-100.000, 100.001-500.000, above 500.000

Check all data collected for this project/purpose:

3. **Identifying numbers:**

Social Security Nr	State ID	Alien Registration	Taxpayer ID	Financial account
Driver's license	Employee ID	Banking ID	Passport number	Patient ID File
Case ID	Credit card	Complaint ID	Tenant ID	Customer ID

Other identifying data (specify):

Purpose of collection:

4. **General personal data**

Name	Date of birth	Place of birth	Maiden name	Religion
Age	Home address	Mailing address	Email address	Telephone Nr.

Military service	Financial info	Gender	Marital status	License plate Nr.
Education level	Schools attended	Citizenship	Former legal name	Social media name

Other general personal data (specify):

Purpose of collection:

5. Work related data

Occupation	Title	Telephone Nr.	Salary	Org. chart level
Email address	Work history	Work address	References	Performance rank

Other work-related data (specify):

Purpose of collection:

6. Distinguishing features/Biometrics

Fingerprints	Photos	DNA profiles	Palm prints	Scars
Marks	Tattoos	Retina/iris scans	Voice recording	Signatures
Vascular scan	Dental profile	Gait analysis	Behavior metrics	Video

Other distinguishing features/biometrics (specify):

Purpose of collection:

7. Sensitive data

Health condition	Disability records	Sexual orientation	Race/Ethnicity	Mental Health
Political affiliation	Voting records	Criminal records	Welfare records	Financial history

Other sensitive data (specify):

Purpose of collection:

8. System admin/audit data

User ID	Login/Passwords	time of access	ID files accessed	IP address
Queries run	Contents of files	MAC address	IMEI/UDID Nr.	Cookies

Other system/audit data (specify):

Purpose of collection:

9. Other data not mentioned in above groups:

Purpose of collection:

Management and Security Measures:

- **Storage Locations**: Specify where each type of data is stored (e.g., physical files, online, encrypted drives, which platform/tool).
- **Access Controls**: List which roles have access to the data and why (focus on need to know and least privilege)
- **Security Measures**: Describe the security measures in place (e.g., encryption, two-factor authentication) for the most sensitive data elements.
- **3rd party sharing:** include conditions of sharing (such as: based on a written contract, with an IT / Legal review) and outline third parties that may have a legitimate reason to access the data. (subcontractor to carry out a specific service or maintenance).
- **Project /data owner:**
- **Retention**: (explain methods of deletion or anonymization after retention period is exhausted)

Review and Update

- **Review Frequency**: Set how often the inventory should be reviewed and updated.
- **Responsible Person**: Identify who is responsible for maintaining the inventory.