**Note**: This toolkit consists of educational materials only and should not be construed as legal advice. Each document needs to be customized to fit the needs of specific entities. Other legal obligations may exist. Please contact the State Privacy Officer at wphillips@utah.gov for further assistance.

**PRIVACY TOOLKIT**

1. **Privacy Notice**: The Utah [Government Data Privacy Act](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19.html) (GDPA) [requires](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S402.html?v=C63A-19-S402_2024050120240501) a *“personal data request notice”* to be provided to individuals at the point of data collection. This template may help you fulfill this requirement. You could also use it for multiple data collections, as long as the document remains simple, specific, and reasonably short.
2. **Breach Notification**: This template is a starting point to providing a notification to affected individuals about a data breach [as required](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S406.html?v=C63A-19-S406_2024050120240501) by the GDPA. It is highly recommended to consult with legal counsel and/or a forensic expert before finalizing this document.
3. **Privacy Policy Statement**: This template is tied to the [Governmental Internet Information Privacy Act](https://le.utah.gov/xcode/Title63D/Chapter2/63D-2.html), which requires entities to have a privacy policy statement on their website, explaining what data is collected and why. You can also find an explainer video on how to implement it [here](https://youtu.be/ebIem10yJzw).
4. **Privacy Policy**: This template is the cornerstone of the GDPA Privacy Program [requirement](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501).
5. **Breach Response:** Find Incident Response documents [here](https://drive.google.com/drive/folders/1ZuXRxc_jSyIjMv05DeM80qYh1Mek2BPw) directly from the Cyber Center.
6. **Training Materials**: This kit includes a [short training video](https://www.youtube.com/watch?v=MiOE1a45iDQ) for new hires, which you can use temporarily before obtaining additional materials from the Data Privacy Office or your own departments/vendors. New hire training is a [direct requirement](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501) of the GDPA.
7. **Personally-Identifiable Information (PII) / Personal Data Inventory**: This tool is linked to data mapping needed to prepare an [annual report](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501) for the State Privacy Officer, as required by the GDPA.
8. **BYOD/Mobile Policy**: If your entity allows the use of personal mobile devices for work, this tool helps implement rules around their use and could be a suitable component of the Privacy Program.
9. **Generative AI Policy**: This policy places safeguards around the use of Generative AI and is a good component of the Privacy Program required by the GDPA.
10. **Information Lifecycle Policy**: This policy sets expectations and rules around the use of information throughout its lifecycle. It is especially useful for larger organizations with complex informational environments and is a valuable component of the Privacy Program.
11. **Privacy Program Outline**: This basic outline shows what a Privacy Program could look like. It is important to customize it to fit your entity's size and needs. Having a codified Privacy Program is a [requirement](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501) of the GDPA.
12. **Privacy Impact Assessment (PIA)**: The GDPA refers to [high-risk processing activities](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S101.html?v=C63A-19-S101_2024050120240501). When you carry out these activities, it’s best practice to use a Privacy Impact Assessment before implementing the project to ensure adequate safeguards are in place for identified privacy risks. Contact the State Privacy Officer for training on how to implement this tool.
13. **Vendor Contract Clauses**: Per GDPA, entities must obligate vendors with access to personal data to meet the same or higher standards. These clauses help you meet that [requirement](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501).
14. **Consent with Data Processing**: Where expressed consent for data processing is required by law, or when collecting optional data, this template helps you capture freely given consent.
15. **Annual Report to State Privacy Officer on Data Sharing Template**: [Required](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501) by the GDPA, this template outlines what should be included in the annual report on data sharing.

**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 Collection Notice Template**

***(this document is related to the*** [***Personal Data Request Notice requirement***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S402.html?v=C63A-19-S402_2024050120240501) ***under The Utah Government Data Privacy Act)***

We [name of organization] are committed to protecting your privacy and handling your data transparently. Below is a summary of the personal information we collect, how we use it, and your rights regarding your data:

**What data do we collect?**

[Describe the data you collect]

Example:

Contact Information: such as your name and email address.

Usage Data: information on how you interact with our services.

Device Information: such as your IP address and browser type.

**Why do we collect this data?**

[Describe the purpose of the collection, be specific, include the record series in which the personal data is or will be included, if applicable.

Example:

To provide and improve our services.

To communicate with you about updates, events, or offers.

For security purposes and to comply with legal obligations.

**Who do we share your data with?**

[Describe the classes of entities you share the data with and who may receive data collected under this notice]

Example: 3rd parties that we contracted with to provide the services you request, such as facilitating payments online.

**How do we protect your data?**

 [Describe in general terms how you protect the data, do not name specific tools or third parties you use]

Example:

We implement adequate security measures including encryption, to ensure the confidentiality and integrity of your data.

**Your rights:**

You can contact us here to carry out your rights:

Example:

Access: You can request to see the data we hold about you.

Correction: You can request that we correct any inaccuracies in your data.

Deletion: You can ask us to delete your data under certain conditions.

Refusal: [describe consequences of refusal to provide the data]

For more detailed information, please visit our [Privacy Policy/ Privacy Policy Statement/ Privacy Program page] (URL). For additional questions contact us here [Email, phone number/ Privacy Officer]

**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 Breach Notification to Impacted Individuals Template**

**This document is related to the** [**breach notification requirement**](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S406.html?v=C63A-19-S406_2024050120240501) **in the Utah Government Data Privacy Act.**

(Date)

To: [Recipient Name]

From: [Your Name]

Dear [Recipient Name],

We are writing to inform you of a recent security incident at [Organization Name]. This notification is sent pursuant to [Utah Code Section 63A-19-406](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S406.html?v=C63A-19-S406_2024050120240501).

**What Happened:** On [Date of Incident], our organization experienced a data breach. During this incident, [brief description of the incident].

**What Information Was Involved:** The breach involved the following categories of personal data: [List specific data categories, e.g., names, addresses, Social Security numbers, etc.].

**What We Are Doing:** We have taken the following steps to address the situation:

1. [Step 1]
2. [Step 2]
3. [Step 3]

**What You Can Do:** To protect yourself from potential identity theft, consider the following actions:

1. **Place a fraud alert** on your credit files. This alerts anyone requesting your credit report that you may be a victim of fraud.
2. **Change passwords** on your email accounts and financial log-ins. Use complex, secure passwords and enable multifactor authentication.
3. **Use a reputable credit monitoring service** to alert you of unusual activity.

Even if you do not find signs of fraud, we recommend regularly reviewing your credit reports from the three major credit reporting agencies. You can obtain a free copy of your credit report once every 12 months by:

* Visiting [www.annualcreditreport.com](http://www.annualcreditreport.com/)
* Calling toll-free at 877-322-8228
* Completing an Annual Credit Request Form at [www.ftc.gov/bcp/menus/consumer/credit/rights.shtm](http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtm)

Additional resources can be found at the Attorney General’s Office at:

<https://attorneygeneral.utah.gov/data-privacy/financial-crimes/>

If you have any questions or need further assistance, please contact [Contact Name] at [Phone Number] or visit [Organization's Website].

Sincerely,

[Title Name] [Signature] [Organization's Representative]

Privacy Policy Statement

 This document is for educational purposes only and does not constitute legal advice.

***(This template is tied to the*** [***Governmental Internet Information Privacy Act***](https://le.utah.gov/xcode/Title63D/Chapter2/63D-2.html)***)***

**In short:**

We care about your privacy, we use the minimal extent of information we need to provide you with services you requested, we safeguard your data and we do not monetize it or improperly share it.

**In detail:**

This Privacy Policy Statement (the "Statement") is provided by [Your Government Entity Name] ("we," "us," or "our") in compliance with Utah Code Section 63D-2-103. We are committed to protecting your privacy. This Statement explains how we handle your information when you visit this webpage. We want you to understand how your data may be collected, used, and secured.

**Who We Are and How to Reach Us**

We operate this governmental website. [If your entity is not the website operator, make that distinction here and include both, your entity as well as the website operator detail]

If you have any questions or concerns, please reach out to us:

By phone: [Provide Telephone Number]

By email: [Provide Email Address]

Our administrative body is [provide your regulator] and they can be reached at [Provide Email Address]

**What Information We Collect**

Here's what we collect when you visit our webpage:

[List the types of personally identifiable information collected, such as name, email, cookies etc.]

**How We Use Your Information**

We use your information for the following purposes:

[Explain how the information is used by us in specific terms, try avoiding vague statements such as “to serve you better”]

**Disclosure Practices**

We care about your privacy. We only share your information when necessary. Here's how we handle disclosures:

[Explain our practices regarding the disclosure of your information, include 3rd parties or categories of 3rd parties you may share the data with and why.]

**Access and Corrections**

You have the right to access and correct your information. Here's how you can do it:

[Describe the steps for users to request access and make corrections in simple terms, provide links if possible]

**Keeping Your Information Secure**

Your data's safety is our priority. We have taken adequate measures to protect it. Here's how we ensure your data stays safe:

[Provide a brief overview of the security measures you have in place; include contractual requirements you place on all your providers]

**Note on Records Classification**

Personally identifiable information is not classification of records under Title 63G, Chapter 2, Government Records Access and Management Act.

Access to government records is governed by Title 63G, Chapter 2, Government Records Access and Management Act.

**Review of this notice**

We want you to feel comfortable using our services, knowing that your privacy is respected and protected and we welcome your feedback on this notice, which is reviewed annually. For more information on our privacy or records management practices click here.

[provide a link to additional policies or procedures that you may have that deal with privacy]

**Last revision:**

[provide date of last revision]

**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***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

**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):

1. **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:

1. **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:

1. **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:

1. **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:

1. **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:

1. **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:

1. **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:

1. 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.

**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.**

**Privacy Policy Simple Template**

***(this document is related to the Privacy Program requirement under The*** [***Utah Government Data Privacy Act***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

***Definitions:***

*Personal Data: information that is linked or can be reasonably linked to an identified individual or an identifiable individual.*

*Processing: any operation or set of operations performed on personal data, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.*

*Sale of data: exchange of personal data for monetary consideration by a governmental entity to a third party.*

**Introduction**

At [Your Organization Name], we prioritize privacy and data security. This Privacy Policy outlines our commitment to safeguarding personal data in compliance with applicable laws and regulations as well as the Utah Fundamental Privacy Principles.

**General Rules:**

Each employee, volunteer, contractor, or other person related to our organization who has access to personal data is obligated to follow this policy and adhere to the Utah Fundamental Privacy Principles.

Each person with access to personal data is obligated, to the best of their ability, to only work with the minimal amount of data needed, and to protect the data they have been entrusted with, to ensure data is not inappropriately shared or exposed and to prevent over-collection and over-retention.

Each person with access to personal data is trained periodically by us, both at the start of their work with us, and on at least an annual basis thereafter.

Each person with access to personal data is responsible for reporting personal data incidents or other adverse events they observe to their manager/dedicated IT or Privacy Officer without delay.

Each person with access to personal data is only allowed to access data to which they have a legitimate need to know and report to their manager/dedicated IT or Privacy Officer if they believe they have wider access than needed.

Persons with access to personal data are not permitted to engage in sale of personal data unless it is required by law. Fees (based on an approved schedule) charged for access to records are not considered sale of personal data.

**Data Collection and Usage**

* We collect and process personal data only for specific, lawful purposes and follow the Utah Fundamental Principles for Data processing. For an overview of the principles see Attachment A. For data inventory information see Attachment B
* Personal data is used solely for the purpose it was collected, unless consent or legal obligations require otherwise.
* We do not sell or otherwise monetize your data.
* Personal data is deleted once its retention period expires and the data is no longer needed.

**Data Access and Sharing**

* Access to personal data is restricted to authorized personnel. You can find more details at (refer to Access Policy).
* We share personal data with third parties only when necessary and in compliance with data protection regulations and under contracts that include necessary data requirements. For a sample of our basic privacy clauses see Attachment C.

**Data Retention**

* We retain personal data only as long as needed for its intended purpose or as legally required.
* (refer to retention schedules/ records retention policy and Records Officer and the process employees should follow to comply.)

**Data Security**

* We employ security measures to protect personal data, including encryption and access controls.
* (describe measures)

**Data Subject Rights**

* Individuals have rights under respective laws, such as GRAMA, that may include access, rectification, erasure, data portability, and objection to data processing rights. For more detail on these rights contact your Privacy/Records Management officer at:

**Data Breach Response**

* We have procedures to detect, report, and respond to data breaches promptly, including notifying affected individuals and authorities.
* (describe procedures high level and refer to more detailed document)

**Privacy Officer**

* Privacy Officer oversees data protection and privacy compliance, monitors the privacy program, responses to data privacy complaints and serves as a point of contact for an individual's privacy rights. Our Privacy Officer can be contacted at: (Provide contact details)

**Information Security Officer:**

* An Information Security Officer (ISO) oversees the protection of an organization’s computers systems and data from cyber threats. They implement security measures, monitor systems for breaches and ensure compliance with security standards and regulations. Our Security Officer can be contacted at: (Provide contact details)

**Training and Awareness**

* Employees and contractors receive training on data protection responsibilities.
* (describe frequency and method on a high level. Recommended is A) within 60 days of new role as well as B) at least once a year. Security and privacy training can be done in one session or module but BOTH have to be addressed, not just cyber security)

 **Compliance Monitoring**

* We regularly review and update privacy policies to ensure compliance with respective laws (enter frequency, recommend is once a year)
* For an example of our monitoring metrics see attachment D

**Questions and Contact Information**

For questions or concerns, contact us at [Contact Information].

**Attachment A**

**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.

**Attachment B**

Personal data notice:

We collect the following data elements for the following purposes and share them with the following classes of people and entities:

**Attachment C**

Sample Privacy Clauses for vendors.

This can be used as a starting point:

<https://auditor.utah.gov/wp-content/uploads/sites/6/2023/08/Privacy-Contract-Clauses-8-29-23.pdf>

**Attachment D**

Overview of recommended monitoring metrics under the Privacy Program:

**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 governmental entity has a properly published privacy policy that the employees or other persons with access to organizations data are required to adhere to Yes/no

2. Designated governmental entity has a privacy policy statement on their website - Yes/No

3. Such statement has been reviewed/updated within the last 12 months - Yes/No

4. Such statement complies with legal requirements outlined in code - Yes/No

5. Designated government entity embeds privacy notices (Data Processing Request Notices) at

entry points of data collection - Yes/No

6. 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 entities take corrective action to ensure that privacy policies are being followed.

Metrics to measure:

1. Health-check conducted within last 24 months - Yes/No,

2. Outcome shows improvement since the last check was performed – Yes/No / N/A

**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 rise 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

6. Annual report provided to the Utah Cyber Center Yes/No

7. Tracking of breaches reportable to the Utah Cyber Center and the Attorney General’s Office is conducted on annual basis: 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 training (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 the 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. The owner of the relationship has been clearly assigned - Yes/No.

5. Third party with access to data are periodically mapped and the results of such mapping is annually reported to the State Privacy Officer.

**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.**

**Bring Your Own Device Policy Template**

***(this document is related to the Privacy Program requirement under The*** [***Utah Government Data Privacy Act***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

**Purpose:**
The purpose of the Bring Your Own Device (BYOD) policy is to allow employees to use their personal devices for work-related activities, enhancing flexibility and productivity, while ensuring that our organization’s data and information remain secure.

**Scope:**
This policy applies to all employees who choose to use their personal laptops, smartphones, or tablets for work-related activities.

**Policy Guidelines:**

1. **Eligibility and Approval:**
	* Employees must receive written approval from their department heads to use personal devices for defined work purposes.
	* Only devices meeting the IT department’s security and compatibility standards will be allowed.
	* Devices must undergo a security and compatibility assessment before approval.
2. **Security Requirements:**
	* Devices must be equipped with up-to-date antivirus software and a secure lock screen.
	* Devices must be updated to the latest operating system version supported by the manufacturer and approved for work purpose.
	* The IT department must install necessary work-related software and configurations, including VPN, encryption tools, and remote wipe capabilities.
	* Multi-factor authentication (MFA) must be enabled on all personal devices used for work.
3. **Mobile Device Management (MDM):**
	* All personal devices used for work must be registered with the company’s MDM system.
	* MDM software will manage the configuration and security of work-related settings and applications.
	* MDM will enable the IT department to remotely wipe company data from the device if it is lost, stolen, or if the employee leaves the company.
	* Employees must agree to the installation of MDM software and regular security updates.
4. **Data Management:**
	* Sensitive or otherwise highly classified data should not be stored locally on personal devices whenever possible.
	* Employees are responsible for backing up personal data. [Company Name] is not responsible for the loss or recovery of personal data on employee devices.
5. **Compliance and Monitoring:**
	* Devices may be subject to periodic audits and compliance checks by the IT department.
	* Devices may be subject to open records requests (GRAMA) or legal discovery actions.
	* Any device that is lost or stolen must be reported to the IT department immediately.
	* Employees must comply with all relevant federal, state, and local regulations regarding data security and privacy.
6. **Acceptable Use:**
	* Personal devices used for work must not be used by anyone other than the authorized employee.
	* Employees must comply with all existing policies regarding the use of technology and the handling of confidential information.
	* Work-related activities on personal devices must adhere to the organization's acceptable use policy.
7. **Termination of Access:**
	* Access to company resources from personal devices can be revoked at any time without prior notice for security reasons.
	* Upon termination of employment, employees must immediately cease using personal devices for work-related purposes and ensure that all company data is completely removed from their devices.
	* Employees must return any organization-provided accessories or peripherals upon termination.
8. **Help and Support**
	* Personal devices and software not utilized for approved work purposes are not eligible to receive support from the governmental agencies’ information technology organization.
	* The employee’s organization will not be held liable for any damage that may occur to personal devices used for work purposes. Employees should have no expectation of repair or replacement for their personal devices. Use of personal devices for work is entirely at the employee’s own risk.
	* Support for work-provided software and applications will be provided through the IT helpdesk.
9. **Cost Reimbursement:**
	* The organization will / will not reimburse employees for the cost of personal devices or their maintenance, repair, or replacement.
	* The organization may reimburse employees for work-related mobile data usage if pre-approved by the department head.
10. **Privacy Considerations:**
	* The organization reserves the right to access, monitor, and review all data and communications on personal devices used for work purposes, in accordance with applicable laws and regulations.
	* Personal data will not be accessed or monitored by the organization unless required by law.

**Acceptance:** Employees must sign an agreement acknowledging that they have read, understood, and agree to abide by the BYOD policy, including the management of their devices through the MDM system.

**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.**

**Generative AI Usage Policy for Governmental Entities Template**

***(this document is related to the Privacy Program requirement under The*** [***Utah Government Data Privacy Act***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

**1. Purpose and Scope**

1.1. This policy outlines the principles and guidelines governing the use of Generative Artificial Intelligence by governmental entities. It aims to promote responsible, ethical, and transparent GenAI deployment to benefit Utah residents and society as a whole.

1.2. Generative AI (GenAI) refers to a class of artificial intelligence systems that are capable of generating content, such as text, images, video, or audio, based on a set of input data rather than simply analyzing or acting on existing data. GenAI technology is rapidly being incorporated into common online tools as standalone systems or embedded within other applications. These systems have the potential to support many state services, however, their use also raises important questions, particularly around the sourcing of training data, ensuring proper attribution of generated content, and the handling of sensitive or public data, accuracy of outputs, bias, and stability.

**2. Ethical and Legal Compliance**

2.1. Governmental entities must adhere to all applicable laws, regulations, and ethical standards when using GenAI. They must respect individuals' rights and privacy, avoid discrimination, and ensure fairness in GenAI-driven decision-making or document producing processes.

2.2. Any GenAI use or deployment that may impact human rights or well-being, such as in public services, should undergo rigorous legal and ethical review, with a Privacy Impact Assessment at its core.

**3. Data Privacy and Security**

3.1. Governmental entities must prioritize data privacy and security when using GenAI. They should implement robust data protection measures and ensure compliance with relevant data protection laws.

3.2. Data used for GenAI training and decision-making must be accurate, up-to-date, and obtained legally. Transparent data management practices should be in place.

3.3. It is of utmost importance that governmental entities do not share any personal, confidential, protected, controlled, or otherwise regulated data with GenAI systems. Generative AI models can produce text or content that may inadvertently disclose sensitive information or create misleading content, and the content is not guaranteed to be kept confidential by the operator or provider of GenAI.

**4. Transparency and Accountability**

4.1. Governmental entities must be transparent about the use of GenAI. Information about GenAI systems, their purpose, and the policies on how the entities use GenAI should be made accessible to the public, where possible.

4.2. Accountability mechanisms should be established to address GenAI-related errors and adverse impacts. Entities must be prepared to rectify issues promptly and respond to requests.

**5. Bias and Fairness**

5.1. Governmental entities must actively mitigate bias and ensure fairness in using GenAI. Continuous monitoring and auditing of the use of GenAI systems for discrimination are essential.

**6. Human Oversight**

6.1. GenAI should assist human decision-makers and not replace them entirely. Human oversight should be maintained in critical decisions, particularly those affecting individuals' rights and liberties.

6.2. Governmental entities should ensure that personnel involved in GenAI deployment receive appropriate training and understand the capabilities and limitations of AI systems, including understanding that GenAI can produce completely false results.

**7. Liability**

7.1. Governmental entities using Gen-AI technologies should establish clear lines of accountability for the decisions made or actions taken by those who rely on GenAI systems.

7.2. Governmental entities should implement appropriate preventative, monitoring and corrective measures to reduce adverse impact resulting from GenAI deployment.

7.3. In the event of errors, or adverse impacts resulting from GenAI deployment, the entity responsible for the use of the GenAI system shall understand they may be found liable for the harm caused.

**8. Review and Revision**

This policy should be reviewed and updated regularly to adapt to evolving GenAI technologies, legal frameworks, and societal expectations.

**9. Dissemination**

This GenAI Usage Policy should be made readily available to all employees and stakeholders within governmental entities and the public.

Effective Date: [Date]

Policy Owner: [Name and Contact Information]

Policy Review Date: [Date for Next Review]

**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.**

**Information Lifecycle Policy Template**

***(this document is related to the Privacy Program requirement under The*** [***Utah Government Data Privacy Act***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

**1. Introduction**

The purpose of this policy is to establish guidelines and procedures for managing the lifecycle of information within [Government Organization Name]. The information lifecycle encompasses the creation, use, storage, and disposal of information to ensure its integrity, security, and compliance with regulatory requirements.

**2. Scope**

This policy applies to all information, regardless of its format or medium, owned or managed by [Government Organization Name].

**3. Definitions**

Information Lifecycle: The progression of information from creation or acquisition through its usage, storage, and eventual disposal.

**4. Information Lifecycle Stages**

*4.1. Creation and Acquisition*

Information Identification: Clearly identify and document the purpose and value of the information to be created or acquired.

Authorship and Ownership: Establish authorship and ownership responsibilities for the creation or acquisition of information.

Metadata and Classification: Assign appropriate metadata and classification to newly created or acquired information for effective management.

*4.2. Storage and Organization*

Storage Infrastructure: Utilize secure and organized storage systems to store information based on its type, sensitivity, and regulatory requirements.

Access Control: Create and Access Control policy, implement appropriate access controls and permissions to ensure that only authorized personnel can access and modify stored information.

Regular Review: Periodically review the stored information to ensure its relevance, accuracy, and compliance with organizational policies.

*4.3. Usage and Distribution*

Authorized Usage: Ensure that information is used for authorized purposes only and in compliance with relevant laws and policies.

Information Sharing: Facilitate secure and controlled sharing of information within and outside the organization while maintaining confidentiality and integrity.

Record Keeping: Maintain accurate records of information usage and distribution for auditing and accountability purposes.

*4.4. Maintenance and Preservation*

Data Integrity: Implement measures to maintain the integrity of information throughout its lifecycle, including backups and version control.

Preservation: Determine the appropriate duration for information preservation based on legal, regulatory, and organizational requirements.

Migration and Conversion: Ensure information remains accessible by planning for migration or conversion to updated formats or systems as technology evolves.

*4.5. Disposal and Destruction*

Data Retention Policies: Define and adhere to data retention policies, specifying the duration for which information will be retained.

Secure Disposal: Implement secure and documented processes for the disposal and destruction of information, ensuring compliance with legal and regulatory obligations.

Documentation of Disposal: Maintain records of information disposal, including the date, method, and reason for disposal.

**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.**

# Governmental Entity Privacy Program Template

***(this document is related to the Privacy Program requirement under The*** [***Utah Government Data Privacy Act***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

## Mission Statement

The Privacy Program is dedicated to ensuring the protection and proper management of personal data within the entity. By adhering to privacy laws and implementing best practices, the program aims to foster a culture of privacy awareness, accountability, and continuous improvement. Our goal is to protect individual privacy rights while enabling the entity to carry out its mission effectively and to follow the state privacy vision and requirements stipulated in the Utah Government Data Privacy Act.

### 1. Introduction

* **Purpose**: Ensure compliance with privacy laws and protect personal data.
* **Scope**: Applies to all employees, contractors, and third parties handling personal data.

### 2. Activities

* **Data Inventory**: Conduct a comprehensive data inventory to identify all personal data collected, stored, and processed.
* **Risk Assessment**: Perform privacy risk assessments to identify potential vulnerabilities.
* **Policy Review**: Review and update privacy policies (Data Retention, Data Access, etc.) regularly.
* **Training and Awareness**: Conduct mandatory privacy training for all employees annually and provide training for new hires within 30 days of their start date.
* **Third-Party Audits**: Assess third-party data handling practices and update agreements as needed.
* **Privacy Impact Assessments (PIA)**: Perform PIAs for new projects or significant changes in data processing or high-risk processing.
* **Security Enhancements**: Implement technical security measures in collaboration with the IT department and the Utah Cyber Security Center and their standards.
* **Data Subject Rights**: Ensure mechanisms are in place for individuals to access, correct, and delete their data.
* **Breach Simulation**: Conduct data breach simulation exercises to test incident response plans.
* **Annual Reporting**:
	+ Prepare and submit an annual report on data sharing to the State Privacy Officer by the end of August.
	+ Prepare and submit an annual report of breaches to the Cyber Center by the end of August.
* **Audit and Compliance Check**: Conduct internal audits to ensure compliance with privacy policies.
* **Review Incident Reports**: Analyze and document any data breaches or incidents and implement corrective actions.
* **Annual Privacy Report**: Prepare an annual privacy report summarizing activities, assessments, and improvements made throughout the year.

### 3. Key Roles and Responsibilities

* **Privacy Officer**: Oversee the privacy program and manage data protection efforts.
* **IT Department**: Implement and maintain technical security measures.
* **Records Management Officer**: Oversee implementation of retention schedules and management of records access requests.
* **Employees**: Adhere to privacy policies and report any privacy incidents.
* **Leadership**: Provide necessary resources and support for the privacy program.
* **Legal counsel**: provide legal advice including classification of incidents and breaches.

### 4. Continuous Improvement

* Regularly review and update the privacy program based on changes in laws, regulations, and best practices.
* Foster a culture of privacy awareness and responsibility within the entity.
* Use a privacy maturity model to assess and improve the program’s maturity, considering factors such as policy implementation, risk management, and incident response capabilities.
* **Responsibility**: The Privacy Officer, in collaboration with Leadership and the Records Management Officer, is responsible for driving continuous improvement.

### 5. Partnerships

* **Attorney General’s Office**: Collaborate for legal guidance and compliance.
* **State Privacy Officer**: Work together to align with state privacy initiatives and reporting requirements.
* **Cyber Center**: Partner for cybersecurity measures and incident management.

### 6. Monitoring Metrics and Maturity Measurement

* **Metrics**: Track the number of data breaches, training completion rates, and compliance audit results, including additional metrics per your privacy policy.
* **Maturity Measurement**: Evaluate the program’s maturity using a privacy maturity model, assessing factors such as policy implementation, risk management, and incident response capabilities.

### 7. Recommended Policies and Standards and Templates

* **Data Retention Policy**: Guidelines for how long different types of data should be retained.
* **Data Access Policy**: Rules for who can access specific types of data and under what conditions.
* **Data Classification Policy**: Framework for categorizing data based on sensitivity and criticality.
* **Breach Notification Policy**: Procedures for reporting data breaches to authorities and affected individuals.
* **Incident Response Plan**: Steps for responding to data breaches or other security incidents.
* **Employee Privacy Training Policy**: Requirements for regular privacy training and awareness programs.
* **Third-Party Data Handling Policy**: Standards for how third parties must manage and protect personal data.
* **Data Minimization Policy**: Practices for collecting only the data necessary for a specific purpose.
* **Encryption Policy**: Guidelines for encrypting sensitive data both at rest and in transit.
* **Privacy by Design and Default Policy**: Ensuring privacy considerations are integrated into all projects and systems from the outset.
* **Individual’s Privacy Rights Policy**: Procedures for enabling individuals to exercise their rights over their personal data.
* **Privacy policy statement -** Document describing data processing practices related to organization’s website.
* **Privacy data request notice:** Document used at data collection for transparency.
* **Consent with Data Processing:**  Document used for processing of personal data where expressed consent is required.

### 8. Contact Information

* Privacy Officer: [Name, Email, Phone Number]

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.

# Basic Privacy Impact Assessment (PIA) Template

***(this document is related to the Privacy Program requirement under The*** [***Utah Government Data Privacy Act***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

**Name of the person filling out the PIA: Entity: Date of PIA:**

**Name of the project**/ **record processing** and its brief description:

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):

1. **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:

1. **Identifying numbers:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Social Security | 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):

1. **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):

1. **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):

1. **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):

1. **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):

1. **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):

1. **Other information** (specify)
2. **Source of the data:** (how was the data obtained): Directly from the person / Indirectly: describe
3. **Purpose for which data is collected:** describe the purpose for the collection and how the collected data is to be used to achieve the primary purpose, indicate if only minimal extent of data is in scope.
4. **Access rights**: list groups/roles that have access to the data throughout their lifecycle, including where the data is stored and how access to it is managed and monitored:
5. **Data sharing with 3rd parties**: describe data sharing and its underlying mechanisms and legal basis.
6. **Notice and consent:** Was notice on data collection provided to the individuals’ prior to the data collection? Y/N Was the data provided based on consent? Y/N Can the consent be easily revoked Y/N? Attach notice language to the report.
7. **Describe measures** (including information security) taken to reduce the risk of unauthorized disclosure:
* **Administrative safeguards** (policies, standards, contract, training, incident response plan...):
* **Physical safeguards** (cabinets, locks, secure doors, CCTV, shredders...):
* **Technical safeguards** (encryption, passwords, 2 factor authentication, firewalls, testing...)
1. **Retention period**: Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period.
2. **Decision making** – are there decisions directly affecting the individual’s privacy rights carried out in connection with this processing? Y/N. If yes, will such decisions be automated Y/N?
3. **Describe any potential threats** to privacy as a result of the use of the information, and mirroring controls that have been put into place to ensure that the information is handled, retained, and disposed of appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule…)

**Evaluation of the PIA carried out by: On:**

Over-collection Y/N, Over-retention Y-N, Suitable Legal bases identified Y/N, Adequate data security methods Y/N, Access rights managed Y/N, Notice/Consent applied Y/N, High Exposure Y/N, High Risk Y/N.

**Pick which one applies**: Inherent privacy risk unmitigated / Inherent privacy risk mitigated inadequately / Residual privacy risk inadequately high / Residual privacy risk adequately controlled.

**Recommendations:**

**APPENDIX 1 TO THE PIA:**

**(to be filled out when scope of project changes)**

## REQUEST FOR NEW USE / DISCLOSURE OF DATA

**Requestor: Responding Entity/ Role: Date:**

Describe the request including its purpose and records in scope:

1. **Would new individuals/groups of individuals have access to the data?** Y/N
* If yes, what individuals/groups of individuals?
* If yes, what data elements would be shared? List all.
1. **Have the individuals whose data is being requested consented** to the new use of their data?
* If yes, was the consent given in writing and was it a stand-alone consent?
* If not, is there a legal basis allowing for such disclosure? If yes, **please specify relevant code**:
1. **How would the data be stored and transmitted**? (describe method including its security)
2. **If new recipients are involved, are they legally or contractually required to keep the data confidential** and securely dispose of it once their purpose has been achieved? Y/N
3. **Can the same purpose be achieved if data is aggregated or anonymized?**
* If yes, what aggregation or anonymization standard will be applied?
* If no, can partial data fulfill the purpose of the request?
* If no, in case of unauthorized access to the full dataset, what is the likelihood of the disclosure causing harm to the individuals? **Pick one**: Very unlikely, Unlikely, Likely, Very Unlikely, Unknown. Examples of harm: public embarrassment, financial loss, reputational loss, identity theft.
1. **Evaluation:**
* Is sensitive or biometric data in scope? Y/N (1/0)
* Was notice and consent for this use/ disclosure provided? Y/N (0/1)
* Is harm likely if data abused? Y/N (1/0)
* Is harm very likely? Y/N (2/0)
* Is such disclosure reasonably expected? Y/N (0/1)
* Are reasonable security controls applied? Y/N (0/1)
* Is there a statement in code allowing such disclosure? Y/N? (0/1)
* Is the data partial, aggregated or anonymized? Y/N (0/1)
1. **Score: 0-8**
	1. 9– use/disclosure can be made, 2 and higher – Privacy, Legal or Records Officer to be consulted.

Privacy Provisions for Vendor Contracts

The following are basic privacy clauses to consider including in third-party contracts when sharing personal, sensitive, confidential, or proprietary data. Review with your legal counsel before use and adjust as needed. This document is for educational purposes only and does not constitute legal advice.

***(this document assists in ensuring 3rd parties comply with the requirements of the*** [***Utah Government Data Privacy Act***](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501)***)***

**Legal Compliance:** The Vendor shall comply with federal and state data protection laws and regulations in relation to the services provided under this contract.

**Data Protection and Security:** The Vendor shall implement and comply with federal and state technical, physical, and administrative regulations to ensure the security and confidentiality of the [contracting party's] data. The Vendor shall employ industry-standard security measures and best practices to safeguard the data. Such measures may include, but are not limited to, encryption, access controls, firewalls, intrusion detection systems, regular security assessments, and employee training on data protection and security.

**Confidentiality:** The Vendor shall maintain the strict confidentiality of the [contracting party's] data and shall not disclose it to any third party without obtaining the [contracting party's] prior written consent. The Vendor shall ensure that its personnel involved in the processing of data are subject to confidentiality obligations and are aware of the importance of maintaining the security of the data.

**Use of Data:** The Vendor shall use the [contracting party's] data solely for the purposes explicitly specified in the contract and may not use the data for any other purpose without obtaining the [contracting party's] prior written consent and is specifically forbidden to sell or otherwise monetize the client’s data.

**Subcontracting:** In the event that the Vendor intends to subcontract any services under this contract, they shall ensure that subcontractors comply with the privacy clauses required by the Vendor and obtain the [contracting party's] approval of the subcontractors engaged.

**Breach[[1]](#footnote-1) Notification:** The Vendor shall promptly notify the [contracting party] within 24 hours of any verified or suspected breach of data security, unauthorized disclosure, or misuse of the [contracting party's] data, as defined by federal and state law. Further, if it is unclear whether an event may be considered a breach, unauthorized disclosure, or misuse of data as defined in the contract, the Vendor shall err on the side of caution and disclose the event to the [contracting party]. The Vendor shall fully cooperate with the [contracting party] during the investigation and mitigation of the breach and shall provide the [contracting party] with all relevant details regarding the breach, including the nature of the breach, the data affected, the potential consequences, and any remedial actions taken or proposed to address the breach. Vendor is obligated to get a [contracting party’s] approval before circulating a notice of breach to the impacted individuals or regulatory bodies.

**Data Deletion:** Upon termination of the contract, the Vendor shall securely delete or return all of the [contracting party's] data as specified in the contract, ensuring that the data is securely and irreversibly deleted to prevent unauthorized access or recovery and providing a Certificate of Destruction within 14 days from contract termination.

**Liability and Insurance:** The Vendor shall assume full liability for any damage or loss arising from a confirmed or suspected breach of data security or privacy, or its investigation, and shall maintain adequate insurance coverage that specifically includes data privacy protection throughout the term of the contract as well as throughout the term the vendor holds or in any way uses the [contracting party’s] data. The Vendor shall provide to the [contracting party] a certificate of insurance satisfactory to the [contracting party] before services provided.

The Vendor acknowledges that its liability for any damage or loss arising from or connected to a data security breach or privacy violation shall not be limited solely to the extent of insurance coverage, and the Vendor remains fully responsible for any liabilities beyond the insurance coverage limits.

**Audit Clause:** The [contracting party] has the right to conduct audits, including on-site, to verify the Vendor's compliance with the contract. The [contracting party] may choose to conduct the audit themselves or engage a third-party auditor, and the Vendor shall fully cooperate with the audit process.

**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 Processing Consent Template**

*(used for optional data or where the law requires expressed consent)*

We [name of your entity] need your permission to use some of your personal information.

Here’s what you need to know:

What We Collect: [describe the types of data you need to collect.]

Why We Need It: [Explain the purpose of processing the data.]

We will not use this data for another purpose, unless you have given us your consent for that purpose as well, or we have a legal basis for processing it, such as to perform a contract with you or as law may from time to time require.

We will only share the data with those that have a legitimate need to know and we will apply appropriate safeguards to your data while under our control. Classes of entities we may share your data with: [describe the classes of people or entities who need access to the data]

Your Choice:

* Yes, I Agree: By selecting this, you allow us to use your information for the purposes described. You can change your mind at any time.
* No, I Do Not Agree: If you prefer not to give consent, we will not process your data for these purposes.

Your Control and Rights: You have control over your data. Contact us at [Contact Email] to change your preferences or ask questions, or request access, correction or deletion of your data, as permitted by law.

**[ ] Yes, I Agree**

**[ ] No, I Do Not Agree**

Name:

Date:

Here is a link to our privacy policy. (put a link to a comprehensive privacy policy)

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.

## Annual Report for Data Sharing and Sales Template

An annual report on data sharing and data sales is required by the Government Data Privacy Act to be submitted to the SPO. We recommend submission by the end of August each year.

This report may be requested via google forms or to be filled out on an interactive portal in the future, stay tuned for further updates from the State Privacy Officer.

**[Government Entity Name]**

**Report to the State Privacy Officer**

**Reporting Period: [Start Date] to [End Date]**

**1. Introduction**

Provide a brief overview of the governmental entity, its mission, and the population it serves.

**2. Types of Personal Data Shared or Sold**

This annual report is prepared in compliance with the Utah Government Data Privacy Act, namely [63A-19-401](https://le.utah.gov/xcode/Title63A/Chapter19/63A-19-S401.html?v=C63A-19-S401_2024050120240501) (2)(i)(i). and aims to provide an overview of personal data sharing practices and potential sales of data incurred during the above mention reporting period.

The following data were shared:

List and describe the categories of personal data shared or sold by the governmental entity during the reporting period.

* **Category 1:** [Description]
* **Category 2:** [Description]
* **Category 3:** [Description]
* **[Additional Categories as needed]**

**3. Basis for Sharing or Selling Personal Data**

Explain the legal, regulatory, or policy basis for sharing or selling each category of personal data. Include references to relevant laws, regulations, or policies.

* **Category 1:**
	+ **Type of transfer: Share / sale**
	+ **Basis:** [Explanation of legitimacy, in case of sale refer to a law that requires it.]
	+ **Reference:** [Law/Regulation/Policy/ approved fee schedule that permits the transfers]
* **Category 2:**
	+ **Type of transfer: Share / sale**
	+ **Basis:** [Explanation of legitimacy, in case of sale refer to a law that requires it.]
	+ **Reference:** [Law/Regulation/Policy/ approved fee schedule that permits the transfers]
* **Category 3:**
	+ **Type of transfer: Share / sale**
	+ **Basis:** [Explanation of legitimacy, in case of sale refer to a law that requires it.]
	+ **Reference:** [Law/Regulation/Policy/ approved fee schedule that permits the transfers]

**4. Classes of Persons and Governmental Entities Receiving Personal Data**

Identify the classes of persons and governmental entities that receive the shared or sold personal data. Provide descriptions, justifications, and underlying administrative mechanisms for these data transfers.

* **Category 1:**
	+ **Recipients:**
		- **Class 1:** [Description]
		- **Class 2:** [Description]
	+ **Governmental Entities:**
		- **Entity 1:** [Description]
		- **Entity 2:** [Description]
* **Category 2:**
	+ **Recipients:**
		- **Class 1:** [Description]
		- **Class 2:** [Description]
	+ **Governmental Entities:**
		- **Entity 1:** [Description]
		- **Entity 2:** [Description]
* **Category 3:**
	+ **Recipients:**
		- **Class 1:** [Description]
		- **Class 2:** [Description]
	+ **Governmental Entities:**
		- **Entity 1:** [Description]
		- **Entity 2:** [Description]

**5. Summary and Recommendations**

Summarize the key points of the report and provide any plans for changes or improvements in your data sharing practices in the upcoming reporting period.

**6. Appendices**

Include any relevant appendices, such as detailed data tables, copies of relevant laws and policies, or additional explanatory materials.

**7. Contact Information**

Provide contact information for the person or office responsible for the report.

* **Name:** [Contact Person]
* **Title:** [Title]
* **Email:** [Email Address]
* **Phone:** [Phone Number]

**Signatures**

* **[Name]**
	+ **Title**
	+ **Date**
1. Breach is typically defined as: the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses regulated data such as personally identifiable information, personal information or personal data, or an authorized user accesses such data for another than authorized purpose. [↑](#footnote-ref-1)