PREPPARATION | PLANNING & ASSESSMENT | EXECUTION & MONITORING

FRAMEWORK APPENDIX

READY SET GO

UTAH OFFICE *of*
DATA PRIVACY

4315 S 2700 W, Taylorsville, UT 84129
officeofdataprivacy@utah.gov | privacy.utah.gov

By December 31, 2025, entities must have initiated their data privacy program. Entities may fulfill this obligation by completing their annual privacy program report by December 31, 2025, and then annually thereafter.[1] When using this Framework as the basis of a privacy program, the Office recommends that entities follow the phases of a simplified "ready, set, go" model, adapted from the NIST Privacy Framework.[2] This approach provides a clear order of operations for creating a new privacy program or maturing an existing one. While an entity is not required to use this model, the Office has included it in this Framework to serve as a helpful resource to guide them through the process. If an entity decides not to follow it, they will need to establish their own systematic approach for their privacy program.

READY

PREPARATION PHASE

1. Designate Responsibility

- Identify and designate an executive-level individual (Chief Administrative Officer (CAO)[3] or a designee) to be responsible for implementing the entity's data privacy program.[4]
- The CAO must appoint one or more records officers or other employees to implement and maintain the data privacy program and its practices.
- The CAO of each governmental entity is required to prepare an annual privacy program report.

SET

PLANNING & ASSESSMENT PHASE

2. Define Program Scope

- Outline the entity's privacy practices to align with both general and entity specific privacy requirements.
- Formalize the data privacy program with a policy, rule, ordinance, or other documentation that details its privacy practices.
- Document whether the entity has initiated a privacy program and any implemented privacy practices in the annual privacy program report.

3. Conduct Maturity Assessment

- Conduct an initial self-assessment using the privacy maturity model to measure the current maturity level of the entity's privacy practices.

4. Identify Strategies

- Based on the maturity assessment, determine strategies that will increase the maturity of specific privacy practices.
- Identify a target maturity level that the entity aims to achieve upon successful implementation of strategies.
- Document any identified strategies in the annual privacy program report.

5. Identify and Prioritize High-Risk Processing Activities

- Based on the maturity assessment, determine strategies that will increase the maturity of specific privacy practices.
- Identify a target maturity level that the entity aims to achieve upon successful implementation of strategies.
- Document any identified strategies in the annual privacy program report.

6. Identify Personal Data Sharing, Selling, or Purchasing

- Create an inventory of the types of personal data the entity shares, sells, or purchases, along with the legal basis for these activities.
- Create a list of the categories of individuals or entities with whom the data is shared, sold, or from whom it is purchased.
- Document both the inventory and the list in the entity's annual privacy program report.

GO

EXECUTION & MONITORING PHASE

7. Implement Prioritized Strategies

- Implement identified strategies to mature the entity's privacy practices.
- After implementing each strategy, update the maturity assessment to reflect the new status of the practice. Creating and prioritizing new strategies should be continuous to further advance privacy maturity.

8. Utilize Privacy Impact Assessments (PIA)

- Use the Office's Privacy Impact Assessment to evaluate new processing activities before implementation to ensure compliance with the GDPA and other applicable privacy requirements.

9. Privacy Awareness Training

- Require all employees to complete the privacy awareness training provided by the Office or an equivalent training created by the entity and approved by the Office.
- Document the percentage of employees who have fulfilled the privacy training requirements in the entity's annual privacy program report.

PATH FORWARD

The Office aims to support entities in initiating their data privacy programs and maturing their privacy practices. The Office anticipates that additional legislative changes will occur to improve privacy laws and move Utah toward alignment with the State Data Privacy Policy[5] in future General Sessions. The practices and efforts outlined in this Framework will be revisited and updated as a new version when appropriate.

Looking forward, the Office views the initiative to increase the maturity of data privacy programs and practices across governmental entities as an ongoing commitment that will involve consistent effort to ensure the privacy programs of governmental entities effectively protect the privacy interests and rights of individuals.

[1] Utah Code § 63A-19-401.3.

[2] https://www.nist.gov/privacy-framework.

[3] Utah Code § 63A-12-100.5(2)(a).

[4] Utah Code § 63A-12-103.

[5] Utah Code § 63A-19-102.