



OFFICE OF THE
STATE AUDITOR

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](#) (GDPA) [requires](#) 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](#) 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](#), 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](#).
4. **Privacy Policy:** This template is the cornerstone of the GDPA Privacy Program [requirement](#).
5. **Breach Response:** Find Incident Response documents [here](#) directly from the Cyber Center.
6. **Training Materials:** This kit includes a [short training video](#) 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](#) of the GDPA.
7. **Personally-Identifiable Information (PII) / Personal Data Inventory:** This tool is linked to data mapping needed to prepare an [annual report](#) 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](#) of the GDPR.
12. **Privacy Impact Assessment (PIA):** The GDPR refers to [high-risk processing activities](#). 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 GDPR, entities must obligate vendors with access to personal data to meet the same or higher standards. These clauses help you meet that [requirement](#).
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](#) by the GDPR, this template outlines what should be included in the annual report on data sharing.