



OFFICE OF THE  
STATE AUDITOR

May 22, 2024

Utah Privacy Commission,

**The State Privacy Officer** (SPO) supports over 1,000 designated governmental entities consisting of more than 225,000 total employees. These entities range from small organizations of a few unpaid volunteers, to large, very complex organizations of over 20,000 employees.

To align with the State Data Privacy policy set out in the Utah Government Data Privacy Act (GDPA) and assist designated governmental entities in fulfilling their privacy obligations, the SPO invites the Utah Privacy Commission to support the following key areas of focus:

- **Attaining compliance:** Creating a feasible strategy for the least mature and least equipped organizations to move toward compliance with Part 4 of the GDPA in an attainable manner within a reasonable timeframe. This may include advocating for legislative adjustments to reflect the disparity in abilities and resources between state agencies and local governments.
- **Training strategy:** Ensuring the Statewide Privacy Awareness Training developed by the newly created Office of Data Privacy includes resources and capacities (e.g., licenses) that cover the entire volume of designated entities, totaling more than 225,000 employees.
- **Cybersecurity resources:** Ensuring the resources produced by the Utah Cyber Center reflect the great diversity of designated entities and enable a customized approach. This means that even entities without in-house cybersecurity expertise or the immediate budget to obtain it externally can benefit from these resources in a way that actually enhances their program maturity.
- **Resource sharing:** Recommending a standard for resource sharing to provide privacy expertise to less mature or resource-limited entities. The SPO can establish tiers of maturity and need based on a risk matrix and continuous risk assessments conducted across the volume of the SPO's scope.
- **Clarification of the GDPA:** Participating in a workgroup proposed by the Chief Privacy Officer (CPO) to steer the body toward providing greater clarity in the GDPA. Considerations may include: a) communicating clear expectations by defining Privacy Program, Covert Surveillance, and Sale of Personal Data, b) removing the current reference to the Government Records Access and Management Act, and c) specifying a timeframe for providing annual reports to the respective bodies, among other additions.
- **New technologies:** Providing ongoing support to emphasizing the transparent, safeguarded and ethical implementation of new technologies, including artificial intelligence. The SPO recommends ensuring human oversight and conducting adequate Privacy Impact Assessments (PIAs) before the implementation of technologies related to high-risk processing becomes a required standard.

Respectfully,  
Dr. Whitney Phillips  
State Privacy Officer