HB 444 DATA PRIVACY AMENDMENTS OVERVIEW

Nora Kurzova & Chris Bramwell

HB 444 Main Objectives

- Clarifies and streamlines terminology.
- Presents a logical placement of privacy related requirements into a more holistic framework.
- Enhances efficiency by restructuring state data privacy governance, with the Office of Data Privacy (ODP) focused on implementation assistance statewide and the State Privacy Auditor (SPA) overseeing compliance.

Key Changes for Governmental Entities

- Removes the requirement for governmental entities to have a fully mature privacy program in place by May 2025 and instead only requires them to initiate a privacy program by July 2025.
- Removes the requirement that a governmental entity report to the Office of Data Privacy and the State Privacy Officer and instead only requires governmental entities to create an internal privacy program report.
- Moves and clarifies the requirements for the completion of a data privacy training program.
- Gives contractors options for the data privacy training they must complete.
- Simplifies the privacy notice a governmental entity must provide to an individual if the personal data collected is a public record.
- Streamlines the website privacy notice, which is now required by Government Internet Information Privacy Act (GIIPA), so governmental entities are required to post information about an individual's privacy rights and the user data collected on their government website.
- Allows a governmental entity to post a notice of a data breach on the governmental entity's government website instead of providing a notice of a data breach directly to an affected person if the personal data involved in the data breach is a public record.

Changes Related to Placement of Requirements:

- Division of Archives and Records Service (DARS) - Title 63A, Chapter 12, Part 1.
- Clarifies the existing requirement for each governmental entity to appoint a Chief Administrative Officer (CAO) and indicates that the CAO is responsible to:
  - Report the name of the governmental entity's CAO and all records officers to Archives.
  - Ensure that the governmental entity complies with the data privacy requirements found in DARS, Government Records Access and Management Act (GRAMA), and the Government Data Privacy Act.
- Moves all the current requirements related to privacy annotations from DARS to the Government Data Privacy Act.

Changes Related to Placement of Requirements *(cont.)*:

- Government Internet Information Privacy Act (GIIPA) - Title 63D, Chapter 2.
- Moves the current requirements for a governmental entity to have privacy notice on their website to the Government Data Privacy Act and moves the:
  - Court website section to the Court's section of the Utah Code at 78A-2-233
  - Authorized domain extension section to the DTS general provisions at 63A-16-110.

Changes Related to the Office of Data Privacy

- Describes that the ODP is required to create a data privacy framework designed to assist governmental entities and to work with governmental entities to study, research, and identify best practices regarding:
  - Automated decision making.
  - The creation and use of synthetic, de-identified, or anonymized data.
  - The use of website tracking technology.
- Allows the ODP to assist governmental entities by creating assessment tools and resources that a governmental entity may use to:
  - Review, evaluate, and mature the governmental entity's privacy program, practices, and processing activities .
  - Evaluate the privacy impact, privacy risk, and privacy compliance of the governmental entity's privacy program, practices, and processing activities.

Changes Related to the State Privacy Officer

- State Auditor Statute - Sections 67-3-1 and 67-3-13.
- Changes the name of the State Privacy Officer to the State Privacy Auditor (SPA).
- Streamlines the duties of the SPA so they are required to:
  - Provide training to all governmental entities on their data privacy auditing standards.
  - Audit all governmental entities, instead of just designated entities.

(with focus on high-risk processing activities including reviewing data sharing and data selling practices.)