Utah Government Privacy Act

Rep. Jefferson Moss

Privacy Drivers

- HB 243 - 2021: Created PPOC, CPO and SPO Roles.
- HB 343 - 2023: Filled gaps in GRAMA, defined PII, annotation requirements.
- OLAG Privacy Audit - 2023: Recommended legislature consider government privacy act to defined privacy guardrails and governance for state agencies.
- Privacy Legislation Working - 2023: Formed to work on proposed privacy legislation.

UGPA Overview

- Initially for state agencies, with future planning for other government entities:
  - Is forward looking, basing compliance requirements on any new PII processing activities;
  - Defines privacy obligations;
  - Establishes data breach and privacy incident reporting requirements;
  - Cleans up existing code and rule to make existing privacy obligations clear;
- Clarifies governance, authorities, accountabilities and responsibilities.
- Creates a privacy request and complaint process for data subjects re: agencies' privacy obligations;
- Creates a Privacy Ombudsman position.

Definitions

Commissioner Smith

(1) "Aggregated data" means information that relates to a group or category of individuals that has been combined into a larger data set such that a person in the data set cannot be individually identified or singled out.

(3) (a) "Biometric data" means data that records an individual's unique biological characteristics that can be used to identify a specific individual.

(b) "Biometric data" includes an individual's:

(i) fingerprint;

(ii) voiceprint;

(iii) eye retinas;

(iv) irises; or

(v) any other unique biological pattern or physical, physiological or behavioral characteristic that can used to identify a specific individual .

(c) "Biometric data" does not include

(i) information captured from a patient in a health care setting; or

(ii) information collected, used, or stored for treatment, payment, or health care operations as those terms are defined in 45 C.F.R. Parts 160, 162, and 164.

(4) "Chief administrative officer" means the highest ranking executive responsible for the administration and operations of a state agency or a person designated by that individual to act as the Chief administrative officer for purposes of this Act, Title 63A, Chapter 12, or Title 63G, Chapter 2.

(5) "Chief privacy officer" means the individual appointed under Section 63A-19-201.

(7) "Data breach" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data, held by a state agency, unless the agency concludes, according to standards established by the Utah Cyber Center, that there is a low probability that personal data has been compromised.

(8) "Data process notice" means notice provided by a state agency that:

(a) meets the requirements of a notice provided by a state agency under Subsection 63G-2-601(2); and

(b) discloses to an individual whether the individual's personal data is expected to bemade public.

(9) "Deidentified data" means personal data that:

(a) has been deidentified such that it cannot be linked to an identified individual or an identifiable individual; and

(b) is possessed by a government entity that:

(i) complies with the standardized process approved by the authority to deidentify the personal data;

(ii) maintains and uses the data only in deidentified form;

(iii) makes no attempt to reidentify the data; and

(iv) contractually obligates any recipients of the data to comply with the requirements described in Subsections (9)(b)(i)-(iii).

(10) "High risk processing activities" means a state agency's processing of personal data that may result in a significant compromise to an individual's privacy interests, based on factors that include:

(a) the sensitivity of the personal data processed;

(b) the amount of personal data being processed;

(c) the individual's ability to consent to the process of personal data;

(d) risks of unauthorized access or use; and

(e) other factors designated by the authority as indicative of a high-risk processing activity.

(11) "Independent entity" means the same as that term is defined in Section 63E-1-102.

(12) "Interested party" means an individual or an individual's legal guardian.

(13) "Ombudsman" means the data privacy ombudsman appointed under Section 63A-19-301.

(14) "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.

(15) "Policy" means a written statement that outlines the principles, guidelines, and goals that direct the activities, operations, and decisions of a state agency.

(16) "Practice" means the specific activities, actions, methods, operations used by a state agency to carry out agency policies and implement programs.

(17) "Procedure" means a state agency's written directions for how policies and practices are implemented in specific situations or tasks to achieve uniformity and consistency in agency operations and outputs.

(18) "Process" means 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.

(19) "Processing activity" means a state agency practice or procedure for processing personal data.

(20) "Publicly available information" means information that a person:

(a) lawfully obtains from a record of a governmental entity;

(b) reasonably believes a consumer or widely distributed media has lawfully made available to the general public; or

(c) if the individual has not restricted the information to a specific audience, obtains from a person to whom the individual disclosed the information.

(21) "Record" means the same as that term is defined in Section 63G-2-103.

(22) "Record series" means the same as that term is defined in Section 63G-2-103.

(23) "Retention schedule" means a state agency's schedule for the retention or disposal of records that has been approved by the Records Management Committee pursuant to Section 63A-12-113.

(24) (a) "State agency" means the following types entities that are under the direct supervision and control of the governor or the lieutenant governor, including:

(i) a department; (ii) a commission; (iii) a board; (iv) a council; (v) an institution; (vi) an officer; (vii) a corporation; (viii) a fund; (ix) a division; (x) an office; (xi) a committee; (xii) an authority; (xiii) a laboratory; (xiv) a library; (xv) a bureau; (xvi) a panel; (xvii) another administrative unit of the state; or (xviii) an agent of an entity described in Subsections (i) through (xviii);

(b) (ii)"State agency" does not include:

(i) the legislative branch;

(ii) the judicial branch;

(iii) an executive branch agency within the Office of the Attorney General, the state auditor, the state treasurer, or the State Board of Education; or

(iv) an independent entity.

(25) "Utah Cyber Center" means the means the Utah Cyber Center created in Section 63A-16-510.

Duties of State Agencies

Chris Bramwell, CPO

State agencies will be required to:

- comply with the provisions of this act unless an agency is subject to a more specific provision of law.
- only process the personal data of an individual in accordance with the provisions of this act and for a lawful purpose.
- Report annually to the authority regarding the state entity's:
  - compliance with all record disposition requirements for every record series maintained by the state agency; and
  - processing of personal data not contained in a record series.

For all new and existing processing activities, state agencies will be required to:

- document the state agency's policies, practices, and procedures for processing and selling personal data;
- dispose of personal data according to the appropriate retention schedule;
- provide notice for changes to purpose and use of personal information previously collected;
- notify an individual when the individual's personal data has been affected by a data breach.

For all <u>new</u> processing activities, state agencies will be required to:

- provide a data process notice to an individual:
  - prior to collecting personal data from the individual; and
  - when a state agency changes the purpose, use, sharing, or legal basis for processing personal data contained in a record series;
- process personal data only for a purpose specified in a data process notice;
- process the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose; and
- not sell personal data unless expressly permitted by law.

Breach Reporting and Notification

Commissioner Sonnenreich

- Agencies will report a data breach affecting 500 or more individuals to the Utah Cyber Center and Attorney General's Office.
- Agencies will maintain incident report documentation of incidents affecting fewer than 500 individuals.
- Agencies will provide notice to individuals affected by a breach. Such notice may include:
  - a description of the data breach;
  - the individual's personal data that was involved in the breach;
  - steps the agency is taking to mitigate the impact of the data breach;
  - recommendations to the individual to protect themselves from identity theft and other financial losses; and
  - any other language required by the Utah Cyber Center.

Data Subject Privacy Request

Chris Bramwell, CPO

- Individuals may submit a data privacy request to state agencies:
  - to obtain information regarding the processing of the individual's personal data;
  - to request an amendment or correction of personal data processed by the state agency; and
  - to request the disposal of personal data according to an approved record schedule.

- Agencies would respond to privacy requests and provide:
  - a unique data privacy request file number;
  - the individual's personal data processed by the state agency;
  - the record series that contains the personal data;
  - the purposes and legal basis for the processing;
  - whether and how the individual's personal data has been shared.

- A state agency that denies a data privacy request would send to the person who filed the data privacy request a written statement containing the legal basis and reasons for the denial.

Data Subject Privacy Complaint

Commissioner Farnsworth

- An individual may file a complaint with the chief administrative officer of the relevant state agency after receiving a response or denial for a data privacy request.

- The complaint would be required to include:
  - the individual's contact information;
  - the data privacy request file number;
  - a description of the alleged violation; and
  - the relief sought.

- An agency would issue a written determination regarding the complaint, alleged violations, and relief sought that is to be provided to the individual.

Data Privacy Ombuds

Commissioner Farnsworth

- Creates a privacy ombudsman.
- A person may submit a request for mediation to the ombudsman any time after submitting a data privacy complaint.
- Mediation would not be required and lack of mediation does not constitute failure to exhaust administrative remedies or bar a legal action.

Utah is recognized nationally for its use of ombuds in providing fair and effective resolution of disagreements, conflicts, complaints, confusion, and questions that inevitably arise in any government. Creation of the privacy ombuds role would be another tool to better resolve privacy issues in the best interest of the residents of Utah and the state government's goals of efficient, effective, and accountable government. Existing Utah ombuds roles include:

- Property Rights Ombuds
- GRAMA Ombuds
- Long Term Care Ombuds
- Child Protection Ombuds

Forward Looking Compliance: Government entities would come into compliance as new processing activities are established or existing processing activities are updated.

Fiscally Sustainable: Government entities would account for the cost of privacy (cost of doing business) in new or substantive changes to existing processing activities. Costs should be required to be estimated and identified in fiscal notes for bills and rules that create new or change existing processing activities. **Entities would not implement <u>new</u> processing activities for which privacy obligations can not be met.**

Transparency: Entities would report non-compliance of pre-existing processing activities to make policy makers aware of resources needed to bring prioritized processing activities into compliance with requirements.