2022

SALT LAKE COUNTY
COUNTY-WIDE POLICY
ON
PERSONAL DATA PRIVACY

Purpose

To ensure that County Agencies collect and process personal data in a manner consistent with the Utah Government Data Privacy Act; Utah Code §§ 63A-19-101 et seq. ("GDPA").

Reference

The Policy and standards set forth herein are provided in accordance with the Utah Government Data Privacy Act; Utah Code §§ 63A-19-101 et seq. Also referencing the following:

Salt Lake County Ordinance Chapter 2.98 - Information Technology Advisory Board
Salt Lake County Policy 2010 GRAMA
Salt Lake County Policy 2020 Records and Information Management
Countywide Information Technology Standard on Cyber Security Incident Reporting and Response
Salt Lake County Standards on Personal Data Privacy (to be created)
Utah Code § 63A-l 9-101 et seq. GDPA

1 Scope

This Policy applies to all Salt Lake County Agencies, employees, and contractors that collect, process or share personal data.

2 Definitions

Some statutory terms are defined here for ease of reference. These and other relevant terms are also defined in the GDPA, Utah Code Title 63A Chapter 19, and the Government Records Access and Management Act ("GRAMA")Title 63G Chapter 2. Clarification may also be offered in Standards developed by the Chief Administrative Officer.

High-risk processing activities means processing of personal data that may have a significant impact on an individual's privacy interests, based on factors that include: (1) sensitivity of the personal data processed; (2) amount of personal data being processed; (3) the individual's ability to consent to the processing of personal data; and (4) risks of unauthorized access or use. "High-risk processing activities" may include the use of (a) facial recognition technology; (b) automated decision making; (c) profiling; (d) genetic data; (e) biometric data; or (f) geolocation data.

Information Technology Resource(s) ("Resource") and/or Information Technology System ("System") means computers, hardware, software, data, storage media,

electronic communications (including, but not limited to, e-mail, fax, phones, phone systems and voice mail); networks, operational procedures and processes used in the collection, processing, storage, sharing or distribution of information within, or with any access beyond ordinary public access to, the County's shared computing and network infrastructure.

Personal Data means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.

Potential Security Incident means an observed event that could potentially compromise the confidentiality, integrity, or availability of the County's Information Technology Resources ("System(s)"). This includes but is not limited to: unusual system behavior, unauthorized access attempts, phishing emails, malware infections, or any activity that deviates from normal operations and may indicate a security threat or breach such as: a missing or stolen County-owned device; an email to a County-email address asking for sensitive information; unusual pop-ups or downloads you didn't authorize on your County-owned device; or anything that seems unusual on a County-owned device, Information Technology Resource or System.

Process, Processing, or Processing Activity 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.

Share or Sharing means providing non public personal data as allowed under GRAMA, Utah Code § 63G-2-206 titled "Sharing Records."

3 Policy Statement

3.1 Salt Lake County recognizes that individuals who provide their personal data to the County have a fundamental interest in, and a reasonable expectation of, privacy regarding that information.

3.2 Accordingly, the Council delegates authority to the Office of Data & Innovation to establish, maintain, and publish standards consistent with this Policy to provide implementation guidance to agencies to implement this Policy.

3.3 All standards established under this Policy shall be reviewed by the Technology Advisory Board which must recommend adoption of the standard before it becomes effective.

3.4 All standards established under this Policy will apply to all individuals who fall within the scope of this Policy.

4 Designation of County's Chief Administrative Officer, Data Coordinators and Data Custodians

4.1 The Office of Data & Innovation Director is designated as the County's Chief Administrative Officer to fulfill the responsibilities set out in Utah Code § 63A-12-103.

4.2 Each Agency shall designate one agency-wide data coordinator. Agencies shall document in writing the name of their designated data coordinator and notify the Chief Administrative Officer of the individual designated. Agency Data Coordinators shall guide their agency's implementation of countywide privacy policies and data governance standards required under the GDPA and as described in the *Data Privacy Standards*.

4.3 Each Agency shall designate at least one Data Custodian for each system the Agency uses to ensure technical management and safeguarding of data. Agencies shall document in writing the names of their designated data custodians and notify the Chief Administrative Officer of the individuals designated. Agency data custodians shall implement system technical safeguards to comply with GDPA and as required in the *Data Privacy Standards*.

5 Privacy Notices – Personal Data Privacy Notice

5.1 Agencies shall provide a privacy notice to individuals from whom they request or collect personal data as outlined below.

5.2 If personal data is requested or collected from a minor or an individual with a legal guardian, the Agency shall provide the notice to the legal guardian.

5.3 **Public Record.** If the Agency is requesting or collecting personal data that would be classified as a public record under GRAMA, Utah Code § 63G-2-301, the privacy notice may be limited to a statement indicating that the individual's personal data may be available to the public as permitted by GRAMA, Utah Code § 63G-2-201.

5.4 **Non-public Record.** If the Agency is requesting or collecting personal data that would not be classified as a public record under GRAMA, Utah Code § 63G-2-301, the privacy notice shall describe:

5.4.1 all intended purposes and uses of the personal data;

5.4.2 the consequences for refusing to provide the personal data;

5.4.3 the classes of persons and governmental entities: a) with whom the Agency shares personal data; or b) to whom the Agency sells personal data; and

5.4.4 the record series in which the personal data is included.

5.5 The Agency shall provide the privacy notice in a manner that individuals providing their personal data are most likely to be aware of the notice. Agencies can consider providing this privacy notice by:

5.5.1 Posting it in a prominent place where the agency collects the data;

5.5.2 Including the notice as part of any document or form used by the agency to collect the personal data; or

5.5.3 Including the notice as part of any document or form used by the agency to collect personal data, a conspicuous link or QR code that links to an electronic version of the privacy notice.

5.6 **Public Safety Data Notice.** When processing personal data to provide emergency services; law enforcement; security cameral monitoring; ambulance and emergency medical services; or 911 emergency communication that serves a public safety interest and produces a public benefit that is greater than or equal to the potential impact on an individual's privacy interest that the notice protects, the Agency shall satisfy its obligations to provide a personal data privacy notice by posting it on their website.

5.7 **Website Privacy Notice.** The Information Technology Division shall prominently post a website privacy notice on the County homepage in compliance with Utah Code § 63A-19-402.5. Any County Agency that operates a separate website under a domain name that is different than the County's official domain shall prominently display a website privacy notice on the homepage of that site.

6 Minimum Reasonable Personal Data Collection

6.1 Agencies may only request and process the minimum amount of personal data from individuals that is reasonably necessary to efficiently achieve the purpose for which it is requested.

6.2 Agencies shall regularly review their data collection practices to ensure compliance with the data minimization requirement.

6.3 Agencies may only use personal data furnished by an individual for the purposes identified in the privacy notice provided to that individual.

7 Privacy Training.

7.1 Agencies shall ensure that employees who have access to personal data as part of their work duties or who supervise an employee who has access to personal data complete the data privacy training offered by the Utah Office of Data Privacy within 30 days after commencement of employment and at least once each calendar year thereafter.

7.2 In addition to the general privacy awareness training, the Office of Data and Innovation and Information Technology Division may create and require employees to complete

Agency-specific privacy training tailored to the unique privacy needs, practices, and requirements of the Agency.

7.3 The Agency Data Coordinator is responsible for monitoring and reporting the completion of data privacy by the employees.

8 Inventorying and Mapping Personal Data Processing Activities.

8.1 For processing activities implemented before May 7, 2025, on or before July 1, 2027, Agencies shall:

8.1.1 Maintain an inventory of all systems used to process personal data.

8.1.2 Maintain an inventory of all records and record series that contain personal data.

8.1.3 Identify the types of data included in the records and records series i.e. public, private, protected, controlled.

8.1.4 Map how the Agency processes personal data they collect from individuals.

8.1.5 Identify whether any processing activities are inconsistent with Section 6.0 of this Policy.

8.1.6 Prepare a strategy for bringing non-compliant processing activities into compliance with the GDPA on or before July 1, 2027.

8.1.7 Agencies shall ensure that all personal data processing activities implemented after May 7, 2025, are subject to the requirements of Section 8.1.1 – 8.1.6 upon implementation.

9 Prohibited Personal Data Processing Activities.

9.1 Unless granted an extension of time to comply or an exemption from compliance from the Utah Office of Data Privacy, Agencies may not:

9.1.1 Establish, maintain, or use undisclosed or covert surveillance of individuals unless permitted by law;

9.1.2 Sell personal data unless expressly required by law; and

9.1.3 Share personal data unless permitted by law.

9.1.4 Agencies must follow GRAMA's Record Sharing provision when sharing personal data. This provision is located at Utah Code § 63G-2-206.

10 Requirements for Contractors

10.1 After July 1, 2026, a contract entered into or renewed with a contractor that processes or has access to personal data as part of the contractor's duties shall contain specific language that requires the contractor to comply with the requirements of Utah Code § 63A-19-401.4

10.2 Contractors are not required to comply with the data privacy training program requirements described in the Utah Code § 63A-19-401.2

11 Amendment or Correction of Personal Data

Agencies that collect personal data shall implement a procedure allowing individuals, or their legal guardians, to request the amendment or correction of personal data, in accordance with applicable laws and regulations.

12 Personal Data Security Incident Reporting and Data Breach Notifications

12.1 Agencies shall adopt and follow the Countywide Information Technology Standard on Cyber Security Incident Reporting and Response to manage and address all security incidents, including data breaches, and privacy violations.

12.2 In the event of a data breach, Agencies shall coordinate with Information Technology Cyber Security Incident Response Team (CSIRT) to issue data breach notices to affected individuals in accordance with Utah Code § 63A-19-406.

13 Privacy Program Report:

13.1 On or before October 31, 2025, and annually on that day thereafter, Agencies shall provide a report to the Office of Data & Innovation including the following information:

13.2 A description of any privacy practices implemented by the Agency and strategies for improving the Agency's privacy practices;

13.2.1 A description of the Agency's high-risk processing activities;

13.2.2 A list of the types of personal data the Agency currently shares, sells, or purchases;

13.2.3 The legal basis for sharing, selling, or purchasing personal data;

13.3 The category of individuals or entities:

13.3.1 with whom the Agency shares personal data;

13.3.2 to whom the Agency sells personal data; or

13.3.3 from whom the Agency purchases personal data;

13.4 The percentage of agency employees that have completed the required privacy training described in this policy;

13.5 A description of any non-compliant processing activities identified under Section 5.0 of this Policy and the agency's strategy for bringing those activities into compliance with this Policy.

14 Periodic Review

14.1 This policy will be reviewed periodically and updated to ensure ongoing compliance with applicable laws and regulations.

APPROVED and PASSED this 23rd day of September, 2025.

SALT LAKE COUNTY COUNCIL

ATTEST:

Lannie Chapman
Salt Lake County Clerk

Reviewed & Advised
as to Form & Legality:
By: */s/ Anneliese Booher*
Anneliese Booher
Deputy District Attorney Date: August 26, 2025