Government Data Privacy - GAA

Policy Application

This policy does not apply to student data, which is governed by Policy FED Student Data Protection, Policy FE Student Records, and the Family Educational Rights and Privacy Act ("FERPA") and related provisions under 20 U.S.C. §§ 1232g and 1232(h). This policy implements the Government Data Privacy Act (Utah Code Title 63A, Chapter 19) and applies to personal data of individuals other than students which is collected and held by the District. This policy applies to all processing (as defined below) implemented by the District after May 1, 2024. For any processing implemented by the District before that date, the District shall, as soon as reasonably practicable but no later than January 1, 2027, identify and document any non-compliant processing activity and prepare a strategy for bringing it into compliance with the Governmental Data Privacy Act.

Utah Code § 63A-19-401(1), (2)(d), (e) (2024)

Definitions

As used in this policy:

1. "Personal data" means information that is linked or can be reasonably linked to an identified individual or an identifiable individual.
2. "Process" or "processing" 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.
3. "High risk processing activities" means processing of personal data by the District 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;
    a. the amount of personal data being processed;
    a. the individual's ability to consent to the processing of personal data; and
    a. risks of unauthorized access or use.
2. "Sell" means an exchange of personal data for monetary consideration by the District to a third party. It does not include a fee charged by the District for access to a record or assessed in accordance with an approved fee schedule.
3. "Data breach" means the unauthorized access, acquisition, disclosure, loss of access, or destruction of personal data held by the District, unless the District concludes, according to standards established by the Utah Cyber Center, that there is a low probability that personal data has been compromised.

Utah Code § 63A-19-101(4), (8), (13), (14), (18) (2024)

Restrictions on Collection and Dissemination of Personal Data

Government Data Privacy - GAA

The District shall obtain and process only the minimum amount of personal data reasonably necessary to efficiently achieve a specified purpose. The District may only use personal data furnished by an individual for the purposes identified in the personal data request notice provided to the individual. The District shall not establish, maintain, or use covert surveillance of individuals unless permitted by law. The District may not sell personal data unless expressly required by law. The District may not share personal data unless expressly permitted by GRAMA or other governing law.

Utah Code § 63A-19-401(1)(b)(ii), (2)(c), (f), (g), (h) (2024)
Utah Code § 63A-19-402(6) (2024)

Annual Report to State Privacy Officer

The District shall annually report to the State Privacy Officer:

1. The types of personal data that the District currently shares or sells;
2. The basis for sharing or selling the personal data; and
3. The classes of persons and the governmental entities that receive the personal data from the District.

Utah Code § 63A-19-401(2)(i)(i) (2024)

Personal Data Request Notice

The District shall provide a personal data request notice to any individual (or for a minor who is not a student, the individual's legal guardian) from whom the District requests or collects personal data. The notice shall include:

1. The reasons the individual is asked to provide the personal data;
2. The intended purposes and uses of the personal data;
3. The consequences for refusing to provide the personal data;
4. The classes of persons and entities that:
    a. Share the personal data with the District or
    a. Receive the personal data from the District on a regular or contractual basis; and
2. The record series in which the personal data is or will be included, if applicable.

The District shall provide the personal data request notice by one of the following means:

1. Posting the notice in a prominent place where the District collects the data;
2. Including the notice as part of a document or form used by the District to collect the data; or
3. Conspicuously linking to or displaying a QR code linked to an electronic version of the notice as part of a document or form used by the District to collect the data.

Upon request, the District shall provide a personal data request notice regarding personal data previously furnished by the individual to an individual (or the individual's legal guardian if the individual is a non-student minor).

Utah Code § 63A-19-402 (2024)

Amendment or Correction of Personal Data

An individual or legal guardian of an individual may request that the District amend or correct personal data about the individual that has been provided to the District. The request shall be in writing and shall specify how the personal data is inaccurate, misleading, or should otherwise be changed. In evaluating the request, the District may ask for further information from the individual requesting the change. The District shall evaluate the request and determine whether the personal data should be amended or corrected and shall inform the requester in writing of the District's determination. A request does not obligate the District to make the amendment or correction sought.

Utah Code § 63A-19-403 (2024)

Data Breach Notification to Individuals

The District shall give notice to an individual affected by a data breach after the District determines the scope of the breach and after restoring the reasonable integrity of the affected system, if necessary. The notice shall be given without unreasonable delay, except that the District shall delay giving notice at the request of a law enforcement agency that determines that notice may impede a criminal investigation. In that case, the notice shall be given when the law enforcement agency informs the District that notice will no longer impede the criminal investigation.

The notice shall include:

1. A description of the data breach;
2. The individual's personal data that was or may have been accessed;
3. Steps the District is taking or has taken to mitigate the impact of the data breach;
4. Recommendations to the individual on how to protect themselves from identity theft and other financial losses; and
5. Any other language required by the Utah Cyber Center.

Unless the District reasonably believes that giving notice would pose a threat to the safety of an individual or unless the individual has designated a preferred method of communication from the District, the District shall provide notice by:

1. Mail or (if reasonably available and allowed by law), email; and
2. One of the following (if the individual's contact information is reasonably available and the method is allowed by law):
    a. Text message, with a summary of the data breach notice and instructions for accessing the full notice; or
    a. Telephone message, with a summary of the data breach notice and instructions for accessing the full notice.

If the data breach affects more than 500 individuals and the District is unable to obtain an individual's contact information to provide notice by one of these methods, the District shall also provide notice of the data breach in a manner that is reasonably calculated to have the best chance of being received by the affected individual or the legal guardian of the

individual, such as through a press release, posting on appropriate social media accounts, or publishing notice in a newspaper of general circulation.

Utah Code § 63A-19-406 (2024)

Data Breach Notification to Utah Cyber Center and Attorney General

The District shall give notice to the Utah Cyber Center and the Utah Attorney General of a data breach that affects 500 or more individuals. The District shall inform the Utah Cyber Center of a data breach that affects fewer than 500 individuals but compromises the security, confidentiality, availability, or integrity of the computer systems used or information maintained by the District. The notice shall be given without unreasonable delay but in any event no later than five days after discovery of the breach.

The notice shall include:

1. The date and time the data breach occurred;
2. The date the data breach was discovered;
3. A short description of the data breach that occurred;
4. The means by which access was gained to the system, computer, or network;
5. The individual or entity who perpetrated the data breach;
6. Steps the District is taking or has taken to mitigate the impact of the data breach; and
7. Any other details requested by the Utah Cyber Center.

If this information is not available within five days of discovering the breach, the District shall provide as much of the information as is available and supplement with additional information as soon as it becomes available.

If the data breach affects 500 or more individuals, the District shall also inform the Utah Cyber Center and the Utah Attorney General of the type of personal data involved in the breach and the total number of people affected by the breach, including the total number of Utah residents affected.

For any data breach that affects fewer than 500 individuals, the District shall as soon as practicable create an internal incident report containing the information required for a notice to the Utah Cyber Center and shall include additional information in this report as it becomes available. These internal incident reports shall be maintained and provided upon request to the Utah Cyber Center. The District shall also provide an annual report to the Utah Cyber Center which logs all the District data breach incidents affecting fewer than 500 individuals.

Utah Code § 63A-19-405 (2024)

Contractor Obligations

Any contractor that enters into or renews a contact with the District and whose duties under the contract include processing personal data shall comply with this policy. The District's contract with such a contractor shall include this requirement.

Utah Code § 63A-19-401(4) (2024)

Staff Training

Each employee of the District whose work duties include access to personal data of individuals shall complete a data privacy training program within 30 days after beginning employment and at least once in each calendar year. The District shall monitor completion of this required training.

Utah Code § 63A-19-401(2)(j), (k), (3) (2024)