Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

UTAH TRANSIT AUTHORITY POLICY

UTA.01.21

DATA PRIVACY

1) Purpose

This policy establishes the principles and practices for protecting Personal Data collected, processed, and stored by the Utah Transit Authority (UTA) in compliance with the Utah Government Data Privacy Act, and where applicable, the General Data Protection Regulation (GDPR), to ensure lawful, ethical, and transparent handling of Personal Data across all UTA operations. It acts as a companion to the Information Security policy and applies to all UTA employees and non-UTA personnel, including outsourced third parties who access UTA's Personal Data This policy applies to all employees, Contractors, and third-party service providers who access or process Personal Data on behalf of the transit agency. It covers all data systems, applications, and processes involving Personal Data. This policy applies to all digital and physical systems, including fare collection, surveillance, mobile applications, websites, and internal databases that store or process Personal Data.

2) Definitions

"Annual Privacy Program Report" means a formal, comprehensive report prepared on a yearly basis that documents UTA's privacy program activities, compliance status, risk assessments, incident response metrics, and improvement initiatives. This report typically includes program governance, compliance activities, metrics and performance, risk management, and planning. The purpose of this report is to demonstrate accountability, support continuous improvement, and provide transparency to the public regarding UTA's privacy posture.

"*CAO*" means Chief Administrative Officer, which is a title for the accountable executive who oversees UTA's privacy program.

"CPO" means the Chief People Officer.

"Cyber Incident Response Standard" means a formal set of documented requirements, procedures, and best practices that govern how UTA prepares for, detects, analyzes, contains, eradicates, and recovers from cybersecurity incidents. This standard ensures a consistent, timely, and effective response to minimize operational, legal, and reputational risks.

"Data/Program Owners" means individuals or designated roles within UTA who hold ultimate accountability for the proper management, protection, and use of specific data sets or programs. They are responsible for ensuring compliance with applicable laws, regulations, and internal policies related to their data or program domain. The Data/Program Owner's functional responsibilities are set forth in Section 3.A.5.

"Data Subject" means an individual whose Personal Data is collected or processed.

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

"DPO" means the Data Protection Officer.

"ECPA" means the Electronic Communications Privacy Act of 1986.

"ET" means the Executive Team, whose functional responsibilities are set forth in Section 3.A.1.

"EU" means the European Union.

"GDPR" means the General Data Protection Regulation.

"GRAMA" means Government Records Access and Management Act, codified at Utah Code Ann.§ 63G-2-101 et seq.

"High-Risk Processing" means Processing that can significantly impact privacy (e.g., biometrics, genetic data, geolocation, profiling, automated decision-making).

"HIPAA" means the Health Insurance Portability and Accountability Act.

"ISO" means the Information Security Office, whose functional responsibilities are set forth in Section 3.A.3.

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

"Personal Data Request Notice" means a formal communication issued by UTA to acknowledge and respond to an individual's request regarding their Personal Data under the applicable privacy laws or internal policies.

"PIA" means Privacy Impact Assessment.

"Privacy-by-Design (PbD)" means taking a foundational approach within technology and system development to embed privacy principles directly into the design and architecture of systems, processes, and technologies from the very beginning. This is a proactive approach to privacy.

"Privacy Framework" means a structured set of principles, standards, and processes that guide UTA's management of Personal Data responsibly and in compliance with applicable laws, regulations, and best practices.

"Privacy Notice" means a statement informing individuals about data collection, use, and rights.

"Privacy Ombudsperson" means an independent, designated individual within or appointed by UTA who serves as an impartial authority for overseeing privacy practices, addressing concerns, and ensuring compliance with applicable data protection laws and internal

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

policies.

"Privacy Steering Committee" means a governance body within an organization responsible for providing strategic direction, oversight, and decision-making related to privacy and data protection. The Privacy Steering Committee ensures alignment between business objectives, regulatory requirements, and privacy best practices.

"Processing" means any operation performed on Personal Data, including collection, storage, use, sharing, or deletion.

"Records Manager" means an individual designated to oversee the creation, maintenance, retention, and disposal of records in compliance with legal, regulator, and organizational requirements, whose functional responsibilities are set forth in Section 3.A.4.

"Records Officer" means an employee that has been appointed by the Executive Director and certified by the Division of Archives and Records Services to Classify UTA's Records.

"Sensitive Data" means biometric data, geolocation, health information, and other data categories as defined by Utah Code §13-61-101.

"Technology Department" means the organizational unit responsible for planning, implementing, and maintaining technology systems, infrastructure, and services that support business operations. This department ensures the secure, efficient, and reliable use of technology resources across the organization, whose functional responsibilities are set forth in Section 3.A.6.

"UODP" means the Utah Office of Data Privacy.

"User Data" means information about a User automatically collected by a UTA website (such as identifiers, IP/MAC, session IDs) when a User visits a UTA website.

"Users" or *"Contractors"* means individuals who are authorized to access, use, or interact with UTA's systems, data, or services, either as internal personnel (users) or external parties engaged under a contractual agreement (contractors). This term encompasses (a) users, meaning employees, temporary staff, or other internal personnel granted access to organizational resources for business purposes, and (b) contractors, meaning third-party individuals or entities performing services under contract, who may require access or systems or data to fulfill their obligations.

"Utah Cyber Center" means the Division of Technology Services in Utah that was created to coordinate efforts between state, local, and federal resources to bolster statewide security and help defend against future cyber-attacks, by sharing cyber threat intelligence and best practices.

"Utah GDPA" means the Utah Government Data Privacy Act.

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

"Utah Office of Data Privacy" means a Utah state agency that was created in the Utah GDPA that works with governmental entities to ensure they effectively protect the privacy interests and rights of individuals.

3) Policy

A. Functional Responsibilities

1. Executive leadership will evaluate and accept privacy risk for UTA, allocate resources as determined in its discretion, support consistent implementation of privacy controls, and ensure compliance with legal obligations.
2. The CAO will develop and maintain the privacy program set forth by executive leadership in compliance with legal obligations, issue notices and standards internally and externally to UTA, oversee PIAs, coordinate privacy incidents and breach notifications among the applicable committees, personnel, and governmental agencies, and prepare the Annual Privacy Program Report.
3. The ISO will align privacy requirements with (a) security architecture within the UTA framework, (b) identity and access management for users, contractors, and the public, (c) logging/monitoring mechanisms within UTA framework, (d) incident response, and (e) vulnerability management.
4. The Records Manager will align privacy annotations and retention schedules and coordinate GRAMA classifications, as classified by a UTA Records Officer.
5. Data/Program Owners will ensure lawful basis and minimum necessary Processing for collecting personal information, maintain data inventories, approve sharing as needed or required, ensure Contractor compliance with this policy and legal obligations, and maintain Privacy Notices.
6. The Technology Department will implement technical controls to ensure compliance with this policy and legal obligations, maintain website Privacy Notices and tracking disclosures, support request workflows, and ensure UTA systems meet Privacy-by-Design requirements.
7. All users or contractors will complete the required training and comply with notices, standards, and procedures.

B. Privacy-by-Design and Minimum Necessary Personal Data

1. When obtaining and Processing Personal Data, it is the standard to only obtain the minimum Personal Data necessary for each specified, lawful purpose.
2. UTA, as a whole, and each division of UTA will embed privacy controls into system design, change management, and vendor selection.
3. To comply with legal obligations and this policy, all collections of Personal Data must document purpose, legal authority, and data elements prior to collection or new Processing.
4. All new systems and vendor contracts must undergo a PIA before deployment. Privacy controls must be embedded in architecture, workflows, and User interfaces.

C. Privacy Governance

1. The Privacy Steering Committee is established by ET to oversee privacy requirements and implementation of such requirements.
2. The Privacy Steering Committee defines escalation paths for privacy concerns, both internally and externally.

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

3. The Privacy Steering Committee includes periodic reviews (at least yearly) and updates to this policy.
4. The Privacy Steering Committee will include periodic reviews (at least yearly) and updates to this policy.

D. Principles
1. *"Data Minimization"* is a principle in data protection and privacy that emphasizes collecting, Processing, and retaining only the minimum amount of Personal Data necessary to achieve a specific purpose. It reduces the risk of data breaches and misuse. This focuses on *how much* data is collected.
2. *"Data Limitation"* is a principle in data governance and privacy that refers to restricting the use, sharing, and retention of data to what is necessary for a specific, legitimate purpose. This focuses on *how* that data is used, shared, and retained.
3. *"Transparency"* in the context of data strategy, governance, and privacy refers to the practice of being open, clear, and honest about how data is collected, used, stored, shared, and protected within UTA. Transparency is a core requirement in regulations like GDPR and HIPAA.
4. *"Security"* refers to the combination of technical and organizational measures that protect personal and Sensitive Data from unauthorized access, breaches, misuse, or loss, while ensuring that individuals' privacy rights are respected. Data is only to be used for the reason it was collected.
5. *"Accountability"* refers to the obligation of organizations and data handlers to take responsibility for how Personal Data is collected, used, protected, and shared. Additionally, Accountability refers to being able to demonstrate compliance with privacy laws, policies, and ethical standards.

E. Data Collection and Use
1. Personal Data must be collected with a Personal Data Request Notice.
2. A notice must be given to individuals (or legal guardians) at the point of collecting indicating how the Personal Data will be used, stored, and retained according to the applicable legal requirements and this policy.
3. Within a public-record data notice given to individuals (or legal guardians), the potential public availability under GRAMA must be indicated.
4. When issued a notice, Data Subjects must be informed of the purpose of the information they provide, the categories of data and how each is treated within UTA's policy, and the rights the Data Subject holds under applicable law and this policy.
5. Data must not sold or shared unless permitted by law.
6. The following list is included in any notice given to an individual (or legal guardian) as necessary for compliance with data collection and use: (a) a website Privacy Notice identity and contact for the Data Subject, (b) access/correction/complaint mechanisms, (c) at-risk employee options, (d) transparency of website tracking technologies, (e) types and uses of User Data, (f) sharing/sale classes, and (g) records series reference.

F. Data Subject Rights

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

1. Access, correction, and deletion rights as set forth in the applicable law to which the Data Subject is subject.
2. All requests from a Data Subject to access, correct, or delete any personally identifying information must be processed within 45 days unless extended.
3. All requests from a Data Subject to access, correct, or delete any personally identifying information must be acknowledged within 10 business days. If this timeline must be extended, justification must be provided to the Data Subject within the 10 business days period.
4. Data Subjects may appeal decisions through the Privacy Ombudsperson.

G. Data Breach Notification and Incident Response
1. Any data privacy or information breaches affecting 500 or more individuals must be reported to the Utah Cyber Center, Attorney General's Office, and any affected individual.
2. Privacy breach events are handled under the Cyber Incident Response Standard.
3. UTA will notify affected individuals without unreasonable delay after scoping and restoring integrity, subject to law-enforcement delay, when applicable.
4. All notifications to affected individuals must include the nature and scope of the breach, and the mitigation steps that have been or will be taken.
5. All privacy breaches must be logged into the incident management system. A post-incident review must be conducted to identify root causes, weaknesses, and preventive actions that may be taken or have been taken to avoid such breaches in the future.

H. High-Risk Processing Activities
1. With regard to High-Risk Processing activities, which include biometric data collection and Processing, geolocation data collection and Processing, and automated decision-making with data collection, a PIA is required.
2. In the case of a High-Risk Processing activity, the applicable division or individual must consult Utah Office of Data Privacy regarding how to approach the activity.
3. The applicable division or individual must also coordinate with ISO to implement safeguards and monitoring as needed.

I. Training and Awareness
1. All personnel, including contractors must complete privacy training within 30 days of hire and annually thereafter.
2. Once the privacy training is completed, it must be tracked and reported in the Annual Privacy Program Report retained by the ISO.
3. Specialized training for high-risk roles (e.g., surveillance, data analytics).

J. Governance and Oversight
1. The ET level position over privacy is responsible for implementation and reporting of privacy and data information within UTA, including, but not limited to, data collection, data breaches, and handling of personally identifying information.

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

2. Where this policy conflicts with other laws, the more specific or restrictive requirement controls.
3. Exceptions may be granted in writing by the CPO in consultation with the ISO when compliance is overly burdensome and equivalent safeguards are in place.
4. Improper use of data or policy violations may result in disciplinary action up to and including termination and, where applicable, referral to law enforcement.
5. The Privacy Framework is maintained in alignment with Utah Office of Data Privacy.

K. GDPR Considerations

If Processing EU resident data, UTA must comply with GDPR, including lawful basis, rights, DPO designation, and cross-border safeguards.

L. Associated Standards

1. Account Management/Access Control Standard
2. Authentication Tokens Standard
3. Security Logging Standard
4. Secure Configuration Management Standard
5. Secure System Development Lifecycle (SSDLC) Standard
6. Sanitization/Secure Disposal Standard
7. Cyber Incident Response Standard
8. Website Privacy Notice Standard (new)

M. Metrics and Reporting

1. All metrics tracked within UTA must be included in the Annual Privacy Program Report submitted to Utah Office of Data Privacy.
2. The metrics tracked and provided must include, but are not limited to:
   a. Number of PIAs completed
   b. Privacy complaints received
   c. Breach incidents

N. Employee Data Handling Guidelines

When handling UTA employee data, the following guidelines must be followed:

1. The collector of the data must ensure responsible handling of employee Personal Data per Utah GDPA, labor laws, and GDPR.
2. The scope of these guidelines applies to all employee-related data, including the data related to Contractors and interns.
3. The categories of employee data include personally identifiable information, employment records, payroll, biometric, communications, emergency contact, etc.
4. Only necessary data may be collected, and such collection must be with notice to the employee and the data may only be used for the reasons stated to the employee.
5. Each employee has the right to access, correct, and delete their stored data, and may request or require data usage transparency.
6. The employee must provide written consent for non-contractual uses of their Personal Data and UTA must document the legal basis for the use of such data.

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

7. Data security includes the requirement that Personal Data is subject to role-based access, encryption, and secure storage.
8. Monitoring or surveillance of employees must be disclosed clearly, limited to legitimate business purposes, and compliant with ECPA and Utah law.
9. Data will only be retained as needed by UTA. Data retention must be followed with clear schedules and secure disposal procedures.
10. Each employee must participate in training within 30 days of hire and annually thereafter. Additionally, enhanced training for Human Resources and IT will be provided.
11. Third-party vendors must sign agreements, comply with UTA-provided standards, and be audited to ensure such compliance, with regard to access to employee Personal Data.
12. Upon the occurrence of any breach of 500 or more employees, the affected employee must be notified of such breach and UTA must report the breach to the proper authorities.

O. Records Retention and Disposal
   1. Any holder of Personal Data must retain and dispose of Personal Data in accordance with approved record retention schedules under UTA's Sanitization/Secure Disposal Standard to systems and media under UTA's Records Management and Access Policy and Records and Information Management - Custodial Responsibilities Procedure.

P. Individual Request to Amend/Correct
   1. A procedure is provided for individuals or legal guardians to request amendments or corrections to Personal Data.
   2. UTA may deny requests for amendment or correction subject to consistency with applicable laws and UTA must document the rationale for the denial.

4) Review and Updates

This policy is effective upon approval by Executive Leadership. This policy is reviewed annually and updated as needed or upon material change in law or operations.

5) Cross-References

- UTA.01.20 Information Security Policy
- UTA.01.08 Records Management and Access Policy
- AGCY.01.08 Records and Information Management - Custodial Responsibilities
- AGCY.01.03 Technology Access Control Standard Operating Procedure
- Cyber Incident Response Standard Utah Code Ann. § 63A-19 Data Privacy Act?
- Website Privacy Notice Sanitization/Secure Disposal Standard.

This standard operating procedure was reviewed by UTA's Chief Enterprise Strategy Officer on 03/03/2026, and approved by the Executive Director on _____. This standard operating procedure takes effect on the latter date.

Docusign Envelope ID: 6A442AB3-5182-4466-A2A9-089FE2763E3D

Jay Fox
Executive Director

Approved as to form and content:

DocuSigned by:
Mike Bell
70E33A415BA44F6...
Counsel for the Authority

History

Date	Action	Owner
	Board Reviewed – UTA.01.21 Data Privacy	Chief Enterprise Strategy Officer
	Adopted – UTA.01.21 Data Privacy	Chief Enterprise Strategy Officer