

TOWN OF BRIGHTON

ORDINANCE NO. 2025-O-12-2

DATE: December 9, 2025

AN ORDINANCE TO INITIATE THE ESTABLISHMENT OF THE TOWN OF BRIGHTON DATA PRIVACY PROGRAM; DESIGNATE CHIEF ADMINISTRATIVE AND AUTHORIZED RECORDS OFFICERS; REQUIRE RECORDS FOR PROOF OF OFFICER AND EMPLOYEE PRIVACY TRAINING; PREPARE WEBSITE DATA PRIVACY NOTICE; ENDORSE THE STATE OF UTAH'S DATA PRIVACY POLICY; AND COMPLETE THE INTERNAL DATA PRIVACY PROGRAM REPORT

WHEREAS, the Town of Brighton Town Council ("**Council**") adopts programs to guide decision-making and policy; and

WHEREAS, the State of Utah requires each governmental entity, including the Town of Brighton ("**Town**"), to initiate a data privacy program ("**DPP**") that recognizes the state policy that "an individual has a fundamental interest in and inherent expectation of privacy regarding the individual's personal data that an individual provides to a governmental entity" and each governmental entity shall process personal data consistent with this state policy pursuant to Utah Code § 63A-19-401; and

WHEREAS, the Utah State Legislature enacted HB 444, Data Privacy Amendments, in 2025, which requires the Town to prepare an internal DPP report ("**Report**") no later than December 31, 2025, pursuant to Utah Code Ann. § 63A-19-401.3; and

WHEREAS, the Council resolves to fully comply with the requirements of Utah Code, Title 63A, Chapter 19, Government Data Privacy Act ("**GDPA**"); Utah Code, Title 63G, Chapter 2, Government Records Access and Management Act ("**GRAMA**"); and Utah Government Operations Code, Title 63A; including the completion of the Report; and

WHEREAS, the Town is a member of the Greater Salt Lake Municipal Services District ("**MSD**") that collects the majority of data from the residents of the MSD member cities and towns for Planning & Development services. The Town supports MSD's own Data Privacy Program as approved by the MSD Board of Trustees; and

WHEREAS, the Council desires to initiate and establish an official Town DPP to be developed and implemented over time to comply with the requirements of Utah Code, Title 63A, Chapter 19, Part 4, Duties of Governmental Entities, and other applicable laws; and

WHEREAS, the Council desires to appoint a Chief Administrative Officer ("**CAO**") and an administrative records officer ("**ARO**") for the City's DPP.

NOW, THEREFORE BE IT ORDAINED by the Town Council of the Town of Brighton, Utah that:

1. Approval of Forms: The Council approves the following forms:

a. The internal privacy report form template included as **Exhibit A** of this Ordinance; and

b. The website data privacy statement attached as **Exhibit B** of this Ordinance.

2. Appointment of CAO: The Council designates Marla Howard as the CAO of the Town DPP and directs the CAO to:

a. Obtain all required training(s); and

b. Oversee the compliance of all Town staff and applicable agents with the data privacy training pursuant to Utah Code § 63A-19-401.2; and

c. Report the names of the designated CAO and ARO to the Division of Archives and Records Services pursuant to Utah Code Subsections 63A-12-103(8)(c)(ii) and 63G-2-108; and

d. Prepare the Report to the best of the CAO's ability using the template attached as Exhibit A in accordance with applicable law and to file the completed report in Town's records, provided that such report will be a protected record; and

e. Prepare the website data privacy statement in a manner that is substantially similar to the notice template attached as Exhibit B and publish the completed statement to the Town of Brighton's official website and the Utah Public Notice Website.

3. Appointment of ARO: The Council designates Kara John, Town Clerk as the ARO of the Town DPP to fulfill all duties under applicable law and Town ordinances and directs the ARO to take all required training(s).

4. Endorsement: The Council endorses the State of Utah's data privacy policy.

5. Enactment of DPP: The Council approves:

a. The initiation and establishment of the Town DPP, with direction to the Mayor and staff to and present to the Council for approval at a later date such other ordinances, rules, or policies needed to implement the DPP and to comply with applicable law; and

b. The designation of the CAO and appointment of the ARO, the intended recordkeeping for proof of completion of ARO training and certification and employee privacy training; and

- c. The preparation and publication of the website data privacy notice; and
- d. The completion of the Report.

6. Additional Direction to Mayor and Staff: The Mayor and staff are authorized and directed to take such other steps as may be needed:

- a. For this Ordinance to become effective under Utah law; and
- b. To make any non-substantive edits to correct any scrivener's, formatting, and numbering errors that may be needed, if any, to this Ordinance.

7. Severability: If a court of competent jurisdiction determines that any part of this Ordinance is unconstitutional or invalid, then such portion of this Ordinance, or specific application of this Ordinance, shall be severed from the remainder, which shall continue in full force and effect.

8. Effective Date: This Ordinance will go into effect immediately.

[execution on following page]

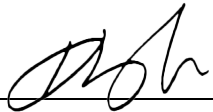
ADOPTED AND APPROVED at a duly called meeting of the Town of Brighton Town Council on this 9th day of December, 2025.

TOWN OF BRIGHTON



By: Dan Knopp, Mayor

ATTEST:



Kara John, Town Clerk



Voting:

Mayor Knopp voting	Aye
Council Member Zuspan voting	Aye
Council Member Brunhart voting	Aye
Council Member Bossard voting	Aye
Council Member Keigley voting	Aye

(Complete as Applicable)

Date ordinance summary was published on the Utah Public Notice Website per Utah Code §10-3-711: 12-12-25

Effective date of ordinance: 12-12-25

EXHIBIT A

Privacy Program Report Template

V1.0_2025.08.01

Disclaimer: This template is provided by the Utah Office of Data Privacy (ODP) as a resource to assist governmental entities. **This template is intended to serve as general guidance and a foundational structure only.** Governmental entities are responsible for reviewing, customizing, and adapting this template to ensure compliance with applicable laws, regulations, policies, and organizational needs.

The ODP makes no representations or warranties, express or implied, regarding the legal sufficiency or suitability of this template for any specific purpose. By using this template, governmental entities acknowledge and agree that the ODP is not liable for the use or modification of this template. **This template is not legal advice and is not a substitute for consultation with legal counsel.** Entities should consult with their own legal counsel before finalizing or executing a document based on this template.

Utah Governmental Entity Privacy Program Report Template v1.0

The Entity must complete a Report, on or before December 31 of each year. The Report should be prepared and certified by the CAO. By completing a Report the Entity has initiated a Program as required by Utah Code § 63A-19-401(2)(a)(i).

Classification: This report is classified as a **protected record** under Utah Code § 63G-2-305, pursuant to Utah Code § 63A-19-401.3(2) and may be made available to the Utah Office of Data Privacy upon request.

Definitions:

- "Governmental entity" means the same as that term is defined in [Subsection 63G-2-103\(12\)](#).
- "High-risk processing activities" means the same as the term is defined in [Subsection 63A-19-101\(17\)](#).
- "Personal data" means the same as the term is defined in [Subsection 63A-19-101\(24\)](#).
- "Privacy practice" means the same as the term is defined in [Subsection 63A-19-101\(26\)](#).
- "Process," "processing," or "processing activity" means the same as the term is defined in [Subsection 63A-19-101\(27\)](#).

- "Purchase" or "purchasing" means the same as the term is defined in [Subsection 63A-19-101\(29\)](#).
- "Sell" means the same as the term is defined in [Subsection 63A-19-101\(33\)](#).

Section 1: Governmental Entity Information

Governmental Entity Name: _____

Governmental Entity Type (Select One):

- | | |
|---|--|
| <input type="checkbox"/> State Agency | <input type="checkbox"/> Interlocal |
| <input type="checkbox"/> County | <input type="checkbox"/> Associations of Government |
| <input type="checkbox"/> Municipality | <input type="checkbox"/> Charter School |
| <input type="checkbox"/> Special Service District | <input type="checkbox"/> Public School |
| <input type="checkbox"/> Board or Commission | <input type="checkbox"/> Independent or Quasi-Government |
| <input type="checkbox"/> College or University | <input type="checkbox"/> Other _____ |
| | _____ |

Mailing Address:

Chief Administrative Officer (CAO):

- **Name:** _____
- **Title:** _____
- **Email:** _____
- **Phone:** _____
- **Date of Report Completion:** _____

Section 2: Privacy Program Status

Fulfills requirement of Subsection 63A-19-401.3(1)(a):

The chief administrative officer of each governmental entity shall prepare a report that includes: **whether the governmental entity has initiated a privacy program.**

A privacy program is the structured collection of a governmental entity's privacy practices, policies, and procedures that govern its processing and protection of personal data to ensure

compliance with applicable laws. A governmental entity's privacy program will meet the December 31, 2025, deadline even if it is not mature or if it is in its early stages, so long as the entity has fully completed its privacy program report or initiated its program through other means that the entity has determined as meeting the requirements of the Government Data Privacy Act.

- Has your governmental entity initiated a **privacy program**?

☐Yes

☐No

- What mechanism(s) has your governmental entity used to initiate its **privacy program**?

☐Administrative Rule

☐Ordinance

☐Resolution

☐Policy

☐Privacy Program Report

Other: _____

Section 3: Privacy Practices, Maturity and Strategies

Fulfills requirement of Subsections 63A-19-401.3(1)(b)(i) and (ii):

The chief administrative officer of each governmental entity shall prepare a report that includes a description of: **any privacy practices implemented by the governmental entity and strategies for improving the governmental entity's privacy program and practices.**

The privacy practices that are listed below are discussed in the Privacy Program Framework v1.0 (Framework), which the Utah Office of Data Privacy created and maintains, and which may be accessed on [Privacy.Utah.Gov](https://www.privacy.utah.gov). The Framework includes privacy practice requirements that are generally applicable of governmental entities as established in the GDPR, Title 63G, Chapter 2, Government Records Access and Management Act (GRAMA), Title 63A, Chapter 12, Division of Archives and Records Service and Management of Government Records (DARSMGR), and some administrative rules. The Framework also includes a maturity model that entities may use to internally assess via this track the maturity of a specific practice and to assist in defining strategies to mature a specific practice. Use of the maturity matrix is not yet required in law, as such, the Office recommends that entities use the maturity matrix because it does tie in with the Framework and other assistance the Office provides. Use will provide a manner for a clear determination of the improvement of an entity's privacy practices and program.

****Entities should revise this section to include other privacy practices that the entity may implement due to entity or data specific laws and regulations.****

Privacy Practice Maturity Model:

Level	Description
Level 0 Non-Existent	The practice is not implemented or acknowledged.
Level 1 Ad Hoc	The practice may occur but is undocumented (no policies or procedures), application is reactive and not standardized.
Level 2 Defined	The practice is implemented and documented, but documentation may not cover all relevant aspects, and application may be informal and inconsistent.
Level 3 Consistently Implemented	The practice is documented to cover all relevant aspects, application is formal and consistent.
Level 4 Managed	The practice is actively managed with metrics that are regularly reviewed to assess efficacy and facilitate improvement.
Level 5 Optimized	The practice is fully embedded in the entity with recognition and understanding across the workforce through active training and awareness campaigns, and inclusion in operations and strategy.

Privacy Practices Implemented:

List all privacy practices implemented, and the strategies your entity will implement, in the coming calendar year to improve its privacy practices and program. The Office recommends entities indicate the current maturity level (0–5) of each practice and select the target maturity they plan to achieve for a given practice by the end of the following calendar year. This will be beneficial to the entity in moving their privacy programs forward.

Governance				
Practice	Implemented	Current	Strategies for	Target

		Maturity	Improvement	Maturity
Gov-1. Chief Administrative Officer (CAO) Designation	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance formally adopting this practice and defines who will make CAO designation and how that designation will be made.	Level 0
Gov-2. Records Officers Appointment	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance formally adopting this practice and defines how the CAO will appoint records officers and review appointments.	Level 0
Gov-3. Records Officer Training and Certification	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance formally adopting this practice and require records officers complete certification.	Level 0
Gov-4. Statewide Privacy Awareness Training	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Gov-5. Privacy Program Report	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Identify				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Ide-1. Record Series Creation and Maintenance	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-2. Record Series Designation and Classification	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-3. Retention Schedule Proposal and Approval	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-4. Record Series Privacy Annotation	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-5. Inventorying	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example strategy:</i> Adopt policy or ordinance that formally adopts this practice.	Level 0
Ide-6. Privacy Impact Assessment	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Ide-7. Record and Data Sharing, Selling, or Purchasing	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0	<i>Example Strategy:</i> Adopt policy or ordinance requiring any sharing, selling or purchasing of data be reported and inventoried.	Level 0

Control				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Con-1. Data Subject Requests for Access	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Con-2. Data Subject Requests for Amendment or Correction	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Con-3. Data Subject Requests for an Explanation	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Con-4. Data Subject Request At-Risk Employee Restrictions	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Communicate				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Com-1. Website Privacy Notice (Policy)	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Com-2. Privacy Notice (Notice to Provider of Information)	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Protect				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
Pro-1. Minimum Data Necessary	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Pro-2. Record Retention and Disposition	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Pro-3. Incident Response	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
Pro-4. Breach Notification	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Other Privacy Practices Implemented by the Governmental Entity				
Practice	Implemented	Current Maturity	Strategies for Improvement	Target Maturity
	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0
	<input type="checkbox"/> Yes <input type="checkbox"/> No	Level 0		Level 0

Section 4: High-Risk Processing Activities

Fulfills requirement of Subsection 63A-19-401.3(1)(b)(iii): The chief administrative officer of each governmental entity shall prepare a report that includes a description of: the governmental entity's high-risk processing activities.

Definition – Utah Code § 63A-19-101(17)(a) and (b):

- (a) **“High-risk processing activities”** means a governmental entity’s processing of personal data that may have a significant impact on an individual's privacy interests, based on factors that include:
 - (i) the sensitivity of the personal data processed;
 - (ii) the amount of personal data being processed;
 - (iii) the individual’s ability to consent to the processing of personal data;
 - and
 - (iv) risks of unauthorized access or use.
- (b) High-risk processing activities may include the use of:
 - (i) facial recognition technology
 - (ii) automated decision making
 - (iii) profiling
 - (iv) genetic data
 - (v) biometric data
 - (vi) geolocation data.

4.1 High-Risk Activities:

Select all applicable high-risk processing activities your entity engages in and provide a brief description of the purposes and uses of each activity.

☐ **Facial recognition technology**

Explanation of Purpose:

☐ **Automated decision making**

Explanation of Purpose:

☐ **Profiling (e.g., behavioral or predictive analysis)**

Explanation of Purpose:

☐ **Genetic data processing**

Explanation of Purpose:

☐ **Biometric data processing (e.g., fingerprints, voice, iris scans)**

Explanation of Purpose:

☐ **Geolocation data processing**

Explanation of Purpose:

4.2 Additional high-risk activities (not listed above):

List any other processing activities your entity has identified as high-risk under the statutory definition and a brief description of the purposes and uses of each.

[Insert narrative or list here]

Section 5: Personal Data Sharing, Selling, and Purchasing

5.1 Personal Data Sharing, Selling, and Purchasing

Fulfills requirements of Subsections 63A-19-401.3(1)(c) and (d):

The chief administrative officer of each governmental entity shall prepare a report that includes: **a list of the types of personal data the governmental entity currently shares, sells, or purchases and the legal basis for sharing, selling, or purchasing personal data.**

Using the checkboxes below identify whether, and the types of, personal data that your governmental entity shares, sells, or purchases and provide a summary of the legal basis for the sharing, selling, or purchasing.

Types of Personal Data	Share, Sell and Purchase Status	Legal Basis for Sharing, Selling or Purchasing
Basic Identification & Contact Information <ul style="list-style-type: none"> ● Full Name ● Date of Birth ● Place of Birth ● Gender ● Age ● Government-Issued Identifiers: <ul style="list-style-type: none"> ○ Social Security Number ○ Driver's License or State ID Number ○ Passport Number ○ Other national or government-assigned IDs ● Contact Information: <ul style="list-style-type: none"> ○ Home Address ○ Email Address(es) ○ Phone Number(s) ○ Mailing Address (if different from home address) 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Demographic & Personal Characteristics <ul style="list-style-type: none"> ● Race or Ethnicity ● Marital Status ● Nationality or Citizenship ● Language Preferences ● Household Information <ul style="list-style-type: none"> ○ Household Size ○ Household Composition 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Employment & Professional Information <ul style="list-style-type: none"> ● Job Title and Position ● Employment History ● Employer Name ● Professional Credentials <ul style="list-style-type: none"> ○ Professional Licenses ○ Certifications ● Work Contact Information 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Financial Data 	<input type="checkbox"/> Share	

<ul style="list-style-type: none"> ● Banking Details <ul style="list-style-type: none"> ○ Bank Account Numbers ○ Credit Card Numbers ● Tax Identification Numbers ● Income and Wage Data ● Credit Information <ul style="list-style-type: none"> ○ Credit Reports ○ Credit Scores ● Payment History 	<input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Health and Medical Information <ul style="list-style-type: none"> ● Medical History ● Diagnoses or Treatments ● Mental Health Data ● Health Insurance Information ● Prescription Information ● Disability Status 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Education Information <ul style="list-style-type: none"> ● School or Institution Attended ● Student ID Numbers ● Academic Records <ul style="list-style-type: none"> ○ Grades ○ Transcripts ● Special Education Status ● Disciplinary Records 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Government Program & Benefits Data <ul style="list-style-type: none"> ● Program Participation (e.g., SNAP, Medicaid, TANF) ● Eligibility Determinations ● Benefit Amounts or Disbursements ● Case Management Notes ● Appeals/Decisions 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Biometric Data <ul style="list-style-type: none"> ● Physical Biometrics <ul style="list-style-type: none"> ○ Fingerprints ○ Facial Recognition Data ○ Retina or Iris Scans ● Voiceprints ● Genetic Information: DNA or other genetic data 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Online & Digital Identifiers 	<input type="checkbox"/> Share	

<ul style="list-style-type: none"> ● Network Identifiers <ul style="list-style-type: none"> ○ IP Addresses ○ Device IDs ● Tracking Technologies <ul style="list-style-type: none"> ○ Cookies ○ Browser Fingerprints ● Location Data (e.g., GPS, precise geolocation) ● Login Credentials (e.g., usernames, hashed passwords) ● Online Activity Logs ● Social Media Handles 	<input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Criminal or Legal Information <ul style="list-style-type: none"> ● Arrest Records ● Conviction History ● Court Records ● Probation or Parole Status ● Incarceration Records 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Vehicle & Property Data <ul style="list-style-type: none"> ● Vehicle Information <ul style="list-style-type: none"> ○ Vehicle Registration ○ VIN Numbers ● Property Ownership <ul style="list-style-type: none"> ○ Property Ownership or Deed Information ○ Property Tax Records ● Utility Usage Data 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Photographic or Video Data <ul style="list-style-type: none"> ● Surveillance Footage ● Government ID Photos ● School or Agency-Provided Photo Records ● Body Camera Footage ● Public Meeting Recordings 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Voting & Civic Data <ul style="list-style-type: none"> ● Voter Registration ● Voting History ● Political District Assignments ● Civic Engagement Program Data 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase	

	<input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Immigration & Travel Information <ul style="list-style-type: none"> ● Visa Status ● Travel History or Itineraries ● Customs Declarations ● Immigration Proceedings 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Communication & Complaints Data <ul style="list-style-type: none"> ● Correspondence <ul style="list-style-type: none"> ○ Emails or Written Correspondence ○ Call Transcripts or Recordings ● Case Notes related to complaints or service requests ● 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<ul style="list-style-type: none"> ● Other Explain: _____ 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	

5.2 Personal Data Recipients and Sources

Fulfills requirements of Subsections 63A-19-401.3(1)(e)(i), (ii), and (iii):

The chief administrative officer of each governmental entity shall prepare a report that includes: **the category of individuals or entities with whom, to whom, and from whom the governmental entity shares, sells, or purchases personal data.**

Mark all that apply:

Processing Activity	Categories of Recipients or Sources
Personal Data Shared With:	Governmental and Public Sector Entities I. Domestic Governmental Entities:

	<input type="checkbox"/> State, Local, Federal, or Tribal Governmental Entities <input type="checkbox"/> Law Enforcement Agencies <input type="checkbox"/> Judicial or Court Systems <input type="checkbox"/> Legislative Bodies or Policy Research Organizations <input type="checkbox"/> Regulatory Agencies <input type="checkbox"/> Professional Licensing Boards II. International Governmental Entities: <input type="checkbox"/> Foreign Governments or International Organizations <input type="checkbox"/> Public Services & Emergency: <input type="checkbox"/> Emergency Services / Disaster Response Agencies <input type="checkbox"/> Public Utilities or Infrastructure Partners III. Public Disclosure: <input type="checkbox"/> Public Disclosure / Open Records Releases Commercial and Private Sector Entities I. Service Providers & Vendors: <input type="checkbox"/> Third-Party Service Providers / Contractors / Vendors <input type="checkbox"/> Cloud Service Providers / Hosting Platforms <input type="checkbox"/> Technology Integrators or Software Developers II. Data & Marketing: <input type="checkbox"/> Private Sector / Commercial Companies <input type="checkbox"/> Data Brokers / Aggregators <input type="checkbox"/> Social Media Platforms III. Financial & Insurance: <input type="checkbox"/> Credit Bureaus or Financial Institutions <input type="checkbox"/> Insurance Providers IV. Healthcare: <input type="checkbox"/> Healthcare Providers or Health Information Exchanges V. Media: <input type="checkbox"/> Media or News Organizations Research, Education, and Nonprofit Entities <input type="checkbox"/> Research Institutions / Universities <input type="checkbox"/> Educational Institutions <input type="checkbox"/> Nonprofit Organizations <input type="checkbox"/> Non-Governmental Watchdogs / Advocacy Groups Individuals and Oversight
--	--

	<input type="checkbox"/> Individuals (e.g., data subjects or their authorized representatives) <input type="checkbox"/> Auditors / Oversight Bodies Other/Not Applicable (N/A) <input type="checkbox"/> Other (Specify as needed) <input type="checkbox"/> N/A (Indicate if no data is shared with or received from any of these categories)
Personal Data Sold To:	Governmental and Public Sector Entities I. Domestic Governmental Entities: <input type="checkbox"/> State, Local, Federal, or Tribal Governmental Entities <input type="checkbox"/> Law Enforcement Agencies <input type="checkbox"/> Judicial or Court Systems <input type="checkbox"/> Legislative Bodies or Policy Research Organizations <input type="checkbox"/> Regulatory Agencies <input type="checkbox"/> Professional Licensing Boards II. International Governmental Entities: <input type="checkbox"/> Foreign Governments or International Organizations <input type="checkbox"/> Public Services & Emergency: <input type="checkbox"/> Emergency Services / Disaster Response Agencies <input type="checkbox"/> Public Utilities or Infrastructure Partners III. Public Disclosure: <input type="checkbox"/> Public Disclosure / Open Records Releases Commercial and Private Sector Entities I. Service Providers & Vendors: <input type="checkbox"/> Third-Party Service Providers / Contractors / Vendors <input type="checkbox"/> Cloud Service Providers / Hosting Platforms <input type="checkbox"/> Technology Integrators or Software Developers II. Data & Marketing: <input type="checkbox"/> Private Sector / Commercial Companies <input type="checkbox"/> Data Brokers / Aggregators <input type="checkbox"/> Social Media Platforms III. Financial & Insurance: <input type="checkbox"/> Credit Bureaus or Financial Institutions <input type="checkbox"/> Insurance Providers IV. Healthcare: <input type="checkbox"/> Healthcare Providers or Health Information Exchanges

	<p>V. Media:</p> <p><input type="checkbox"/> Media or News Organizations</p> <p>Research, Education, and Nonprofit Entities</p> <p><input type="checkbox"/> Research Institutions / Universities</p> <p><input type="checkbox"/> Educational Institutions</p> <p><input type="checkbox"/> Nonprofit Organizations</p> <p><input type="checkbox"/> Non-Governmental Watchdogs / Advocacy Groups</p> <p>Individuals and Oversight</p> <p><input type="checkbox"/> Individuals (e.g., data subjects or their authorized representatives)</p> <p><input type="checkbox"/> Auditors / Oversight Bodies</p> <p>Other/Not Applicable (N/A)</p> <p><input type="checkbox"/> Other (Specify as needed)</p> <p><input type="checkbox"/> N/A (Indicate if no data is shared with or received from any of these categories)</p>
<p>Personal Data Purchased From:</p>	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities:</p> <p><input type="checkbox"/> State, Local, Federal, or Tribal Governmental Entities</p> <p><input type="checkbox"/> Law Enforcement Agencies</p> <p><input type="checkbox"/> Judicial or Court Systems</p> <p><input type="checkbox"/> Legislative Bodies or Policy Research Organizations</p> <p><input type="checkbox"/> Regulatory Agencies</p> <p><input type="checkbox"/> Professional Licensing Boards</p> <p>II. International Governmental Entities:</p> <p><input type="checkbox"/> Foreign Governments or International Organizations</p> <p><input type="checkbox"/> Public Services & Emergency:</p> <p><input type="checkbox"/> Emergency Services / Disaster Response Agencies</p> <p><input type="checkbox"/> Public Utilities or Infrastructure Partners</p> <p>III. Public Disclosure:</p> <p><input type="checkbox"/> Public Disclosure / Open Records Releases</p> <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors:</p> <p><input type="checkbox"/> Third-Party Service Providers / Contractors / Vendors</p> <p><input type="checkbox"/> Cloud Service Providers / Hosting Platforms</p> <p><input type="checkbox"/> Technology Integrators or Software Developers</p> <p>II. Data & Marketing:</p>

	<input type="checkbox"/> Private Sector / Commercial Companies <input type="checkbox"/> Data Brokers / Aggregators <input type="checkbox"/> Social Media Platforms III. Financial & Insurance: <input type="checkbox"/> Credit Bureaus or Financial Institutions <input type="checkbox"/> Insurance Providers IV. Healthcare: <input type="checkbox"/> Healthcare Providers or Health Information Exchanges V. Media: <input type="checkbox"/> Media or News Organizations Research, Education, and Nonprofit Entities <input checked="" type="checkbox"/> Research Institutions / Universities <input type="checkbox"/> Educational Institutions <input type="checkbox"/> Nonprofit Organizations <input type="checkbox"/> Non-Governmental Watchdogs / Advocacy Groups Individuals and Oversight <input type="checkbox"/> Individuals (e.g., data subjects or their authorized representatives) <input type="checkbox"/> Auditors / Oversight Bodies Other/Not Applicable (N/A) <input type="checkbox"/> Other (Specify as needed) <input type="checkbox"/> N/A (Indicate if no data is shared with or received from any of these categories)
--	--

Section 6: Privacy Training Completion

Fulfills requirement of Subsection 63A-19-401.3(1)(f):

The chief administrative officer of each governmental entity shall prepare a report that includes: **the percentage of the governmental entity's employees that have fulfilled the data privacy training requirements described in Section 63A-19-401.2.**

What percentage of your entity's employees have completed the required privacy training requirements described in Section 63A-19-401.2?

Section 7: Non-Compliant Processing Activities (Must be completed by Dec 31, 2027)

Fulfills requirement of Subsections 63A-19-401(2)(a)(iv)(D) and 63A-19-401.3(1)(g):

The chief administrative officer of each governmental entity shall prepare a report that includes: **a description of any non-compliant processing activities identified under Subsection 63A-19-401(2)(a)(iv) and the governmental entity's strategy for bringing those activities into compliance with Part 4 of the Government Data Privacy Act.**

Have any non-compliant processing activities been identified pursuant to Utah Code § 63A-19-401(2)(a)(iv)?

☐ *Yes*

☐ *No*

If yes, provide details:

Processing Activity Name	Processing Activity Type	Issues Identified	Strategies for Compliance	Estimated Completion Date

Certification

Certification must be completed by the governmental entity's chief administrative officer.

I, the undersigned, certify that the information provided in this report is accurate to the best of my knowledge.

Name: _____

Signature: _____

Date: _____

EXHIBIT B

Town of Brighton Website Privacy Notice

Introduction

Thank you for visiting the Town of Brighton (“Brighton,” “we,” or “our”) website. We are committed to protecting your personal information and your right to privacy. If you have any questions about this privacy statement or our practices about your personal information, please contact **Maridene Alexander** at Maalexander@msd.utah.gov.

What information do we collect?

In short: We collect personal information that you voluntarily provide to us and information that is automatically collected.

1) Information You Provide to Us.

We collect personal information that you voluntarily provide to us when you express an interest in obtaining information about us or our products and services, when you participate in activities on the website or otherwise when you contact us. Personal information shall be defined as consistent with Utah Code 13-44-102.

The personal information that we collect depends on the context of your interactions with us and the Website, the choices you make, and the products and features you use. The personal information we collect may include the following:

Payment Data. We may collect data necessary to process your payment if you make payments for services provided by the Greater Salt Lake Municipal Services District (“MSD”). Please note, the MSD contracts with third-party vendors to collect and process online payments for business licenses, building permits, planning applications and parking ticket fines. These vendors collect information from you voluntarily when you register or initiate online payment transactions through their websites. They collect your name, address, email, phone number and credit/debit card number, card issue date, and the security code associated with your payment instrument. You may find their privacy notice here:

- Xpress Bill Pay - <https://www.xpressbillpay.com/privacy/>
- Cityworks – <https://www.cityworks.com/legal/privacy-policy/>

All personal information you provide must be true, complete, and accurate, and you must notify us of any changes to such personal information.

2) Information Automatically Collected.

We automatically collect certain information when you visit, use, or navigate the Website. This information does not reveal your specific identity (like your name or contact information) but may include device and usage information, location data, or website visitor information.

- **Device Data** – such as your IP address (or proxy server), browser and device characteristics (name, identification numbers, operating system), internet service provider and/or mobile carrier, type of device, language preferences, referring URLs, usage patterns and preferences as you navigate the Website.
- **Location Data** – such as device location, PGS and other technologies to collect geolocation data that tells us your approximate location (based on your IP address). You can opt out of allowing us to collect this information by refusing access to the information or by disabling your location settings on your device.
- **Website visitor information** – we may collect information about how and when you visit the Website about your visit, such as pages you visited and when you use the Website and other information for our internal analytics and reporting purposes.

We contract with CivicPlus to be the Website content management system for Brighton. Here is a link to their privacy policy: <https://www.civicplus.com/privacy-policy/>

We contract with Esri to use its Geographic Information System (GIS) IS system for mapping and analyzing data. Here is a link to the ESRI Privacy Policy: <https://www.esri.com/en-us/privacy/privacy-statements/privacy-statement>

How do we use your information?

In short: We process your information for purposes based on legitimate business interests, the fulfillment of our service with you, compliance with our legal obligations, and/or your consent.

We use personal information collected via the MSD Website for a variety of business purposes described below. We process your personal information for these purposes in reliance on our legitimate business interests, in order to provide you with a service, a license, a permit, or other information, with your consent, and/or for compliance with our legal obligations.

We use the information we collect or receive:

- To fulfill service obligations.
- To personalize the user experience on the Website.
- To improve customer service.
- To send periodic emails.

- To respond to your inquiries or offer support to users.
- To provide you with a license or a permit needed to conduct business or build or modify a business or home.
- To send administrative information to you.
- To enforce our terms, conditions and policies for business purposes, to comply with regulatory requirements or in connection with our contract.
- To respond to legal requests and prevent harm.

Will your information be shared with anyone?

In short: We only share information with your consent, to comply with laws, to provide you with services, to protect your rights, or to fulfill business obligations.

We may process or share the data that we hold based on the following legal basis:

- **Consent:** We may process your data if you have given us specific consent to use your personal information for a specific purpose.
- **Legitimate Interests:** We may process your data when it is reasonably necessary to achieve our legitimate business interests.
- **Performance of a Service:** Where we are providing a service to you, we may process your personal information to fulfill the request for a permit, license, approval or other such purpose.
- **Legal Obligations:** We may disclose your information where we are legally required to do so in order to comply with applicable law, governmental requests, a judicial proceeding, court order, or legal process, such as in response to a court order or a subpoena, consistent with Utah Code Sections 77-23c-101 to 77-23c-105.
- **Vital Interests:** We may disclose your information where we believe it is necessary to investigate, prevent, or take action regarding potential violations of our policies, suspected fraud, situations involving potential threats to the safety of any person and illegal activities, or as evidence in litigation in which we are involved.

How long do we keep your information?

In short: We keep your information for as long as necessary to fulfill the purposes outlined in this privacy notice unless otherwise required by law.

Brighton and the MSD will only keep your personal information for as long as it is necessary for the purposes set out in this privacy notice unless a longer retention period is required or

permitted by law (such as tax, accounting, or other legal documents). No purpose in this notice will require us to keep your personal information for longer than three years.

When Brighton and the MSD has no ongoing legitimate business need to process your personal information, we will either delete or anonymize such information, or, if this is not possible (for example, because your personal information has been stored in backup archives), then we will securely store your personal information and isolate it from any further processing until deletion is possible, consistent with Utah Code 13-44-201.

- We retain personal data only as long as necessary to fulfill the purposes outlined in this privacy statement unless a longer retention period is required or permitted by law. (such as tax, accounting or other legal documents).
- No purpose in this statement will require us to keep your personal information for longer than three years.
- Deletion schedule: consistent with Utah Code 13-44-201.

How do we keep your information safe?

In short: We aim to protect your personal information through a system of organizational and technical security measures.

We have implemented appropriate technical and organizational security measures designed to protect the security of any personal information we process. However, despite our safeguards and efforts to secure your information, no electronic transmission over the internet or information storage technology can be guaranteed to be 100% secure, so we cannot promise or guarantee that unauthorized third parties will not be able to defeat our security, and improperly collect, access, steal, or modify your information.

Although we will do our best to protect your personal information, transmission of personal information to and from our Website is at your own risk. You should only access the Website within a secure environment. If we become aware of a security breach we will notify you pursuant to Utah Code Section 13-44-202.

What are your privacy rights?

In short: You may review, change, or terminate your account at any time.

Individuals have rights under respective laws, such as GRAMA, that may include access, rectification, erasure, data portability, and objection to data processing rights. For more detail on these rights contact your Privacy/Records Management officer at: Marla Howard at mahoward@msd.utah.gov

How do we respond to a data breach?

In short: We have procedures to detect, report, and respond to data breaches promptly, including notifying affected individuals and authorities.

How do we make updates to this notice?

In short: Yes, we will update this notice as necessary to stay compliant with relevant laws.

We regularly review and update privacy policies to ensure compliance with respective laws. We will update this policy as necessary to stay compliant with relevant laws. We reserve the right, at our discretion, to change, modify, add, and/or remove portions of the Privacy Policy at any time.

How can you contact us about this notice?

If you have questions or comments about our Privacy Policy Statement, you may email us at Maalexander@msd.utah.gov

Last updated: 11/21/2025