

ORDINANCE NO. 591

DATE: 1-21-26

AN ORDINANCE TO INITIATE THE ESTABLISHMENT OF THE CARBON COUNTY 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 CARBON COUNTY'S INTERNAL DATA PRIVACY PROGRAM REPORT.

WHEREAS, Carbon County ("**County**") adopts programs to guide decision-making and policy; and

WHEREAS, the State of Utah requires each governmental entity, including County to initiate a data privacy program ("**DPP**") that recognizes the state policy that "an individual has 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 County 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 County 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 County desires to initiate and establish an official County 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 County desires to appoint a Chief Administrative Office ("**CAO**") and an administrative records officer ("**ARO**") for the County's DPP.

NOW, THEREFORE BE IT ORDAINED by that:

1. **Approval of Forms:** The County 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 County designates Kellie Payne, Carbon County Human Resource Director, as the CAO of the County DPP and directs the CAO to:
 - a. Obtain all required training(s); and
 - b. Oversee the compliance of all County 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 County'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 County's official website and the Utah Public Notice Website.
3. **Appointment of ARO:** The County designates Sophia Jones and Tess Tonc as the ARO's of the County DPP to fulfill all duties under applicable law and County ordinances and directs the ARO to take all required training(s).
4. **Endorsement:** The County endorses the State of Utah's data privacy policy.
5. **Enactment of DPP:** The County approves:
 - a. The initiation and establishment of the County DPP, to present to the County for approval at a later date such other ordinances, rules, or policies needed to implement the DPP and to comply with the 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 Staff:** The 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]

**SUMMARY OF
Carbon County
ORDINANCE NO. 591**

On January 21, 2026, the County enacted Ordinance No. 591 to: (1) establish a data privacy program per H.B. 444; (2) designate chief administrative and authorized records officers; (3) require records for proof of officer and employer privacy training; (4) prepare a website data privacy notice; (5) endorse the State of Utah's data privacy policy; and (6) complete and initial data privacy program report.



Jared Haddock, Carbon County Commission Chair

ATTEST:



Seth Marsing, Carbon County Recorder

ADOPTED AND APPROVED at duly called meeting of Carbon County Commission on this
21 day of January, 2026.



Jared Haddock, Carbon County Commission Chair

ATTEST:



Seth Marsing, Carbon County Auditor

(Complete as Applicable)

Date ordinance summary was published on the Utah Public Notice Website per Utah Code §

10-3-711: 1-28-2026 Loni Hawk

Effective Date of Ordinance: 1-21-2026

Exhibit A

SECTION 1: GOVERNMENTAL ENTITY INFORMATION

Name: _____

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"/> Special District |
| <input type="checkbox"/> Board or Commission | <input type="checkbox"/> Independent or Quasi-Government |
| <input type="checkbox"/> College or University | <input type="checkbox"/> Public School |
| <input type="checkbox"/> Other _____ | |

Mailing Address: _____

Chief Administrative Officer (CAO):

Name: _____

Title: _____

Email: _____

Phone: _____

SECTION 2: PRIVACY PROGRAM STATUS

The Report must include whether the governmental entity has initiated a privacy program. (Utah Code § 63A-19-401.3(1)(a)) 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 (GDPA).

Has your governmental entity initiated a privacy program?

☐ Yes

☐ No

How has the governmental entity initiated a privacy program?

☐ Administrative Rule

☐ Ordinance

Resolution

☐ Policy

☐ Privacy Program Report

☐ Other _____

SECTION 3: PRIVACY PRACTICES, MATURITY AND STRATEGIES


The Report must include any privacy practices implemented by the governmental entity and strategies for improving the governmental entity's privacy program and practices. (Utah Code § 63A-19-401.3(1)(b) (i) and (ii)). The privacy practices listed below are discussed in the Privacy Program Framework (Framework), which the Office created and maintains, and which may be accessed on privacy.utah.gov. The Framework includes privacy practice requirements that are generally required by governmental entities as established in the GDPA, 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 the maturity of a specific practice and create strategies to mature a specific practice. Although using the maturity matrix is not required at this time, the Office recommends that entities use the maturity matrix in conjunction with the Framework and other assistance the Office provides. Any other applicable privacy practices required by sector specific laws or regulations should also be included.

PRIVACY MATURITY MODEL



PRIVACY PRACTICES IMPLEMENTED:

Check all privacy practices the governmental entity has implemented so far, and describe the strategies the governmental entity will use 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 governmental entity in moving their privacy programs forward.

 GOVERN				
PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
1.1 Chief Administrative Officer (CAO) Designation	<input type="checkbox"/> Yes <input type="checkbox"/> No			
1.2 Records Officers Appointment	<input type="checkbox"/> Yes <input type="checkbox"/> No			


1.3 Records Officer Training and Certification	<input type="checkbox"/> Yes <input type="checkbox"/> No			
1.4 Statewide Privacy Training	<input type="checkbox"/> Yes <input type="checkbox"/> No			
1.5 Privacy Program Report	<input type="checkbox"/> Yes <input type="checkbox"/> No			

IDENTIFY

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
2.1 Record Series Creation and Maintenance	<input type="checkbox"/> Yes <input type="checkbox"/> No			
2.2 Record Series Designation and Classification	<input type="checkbox"/> Yes <input type="checkbox"/> No			
2.3 Statement Filed with State Archivist	<input type="checkbox"/> Yes <input type="checkbox"/> No			

2.4 Retention Schedule Proposal and Approval	<input type="checkbox"/> Yes <input type="checkbox"/> No			
2.5 Record Series Privacy Annotation	<input type="checkbox"/> Yes <input type="checkbox"/> No			
2.6 Inventorying	<input type="checkbox"/> Yes <input type="checkbox"/> No			
2.7 Privacy Impact Assessments (PIA)	<input type="checkbox"/> Yes <input type="checkbox"/> No			

2.8 Record and Data Sharing, Selling, or Purchasing	<input type="checkbox"/> Yes <input type="checkbox"/> No			
---	---	--	--	--


 CONTROL				
PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
3.1 Data Subject Requests for Access	<input type="checkbox"/> Yes <input type="checkbox"/> No			
3.2 Data Subject Requests for Amendment or Correction	<input type="checkbox"/> Yes <input type="checkbox"/> No			

3.3 Data Subject Requests for an Explanation	<input type="checkbox"/> Yes <input type="checkbox"/> No			
3.4 Data Subject Request by At-Risk Employees for Restricting Access	<input type="checkbox"/> Yes <input type="checkbox"/> No			

COMMUNICATE

PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
4.1 Privacy Notice (Notice to Provider of Information)	<input type="checkbox"/> Yes <input type="checkbox"/> No			

4.2 Website Privacy Notice and Website Privacy Policy	<input type="checkbox"/> Yes <input type="checkbox"/> No			
---	---	--	--	--

 PROTECT				
PRACTICE	IMPLEMENTED	CURRENT MATURITY	STRATEGIES FOR IMPROVEMENT	TARGET MATURITY
5.1 Minimum Data Necessary	<input type="checkbox"/> Yes <input type="checkbox"/> No			
5.2 Retention and Disposition of Records Containing Personal Data	<input type="checkbox"/> Yes <input type="checkbox"/> No			

5.3 Incident Response and Notification to the Cyber Center and Attorney General	<input type="checkbox"/> Yes <input type="checkbox"/> No			
5.4 Breach Notification to Affected Individuals	<input type="checkbox"/> Yes <input type="checkbox"/> No			

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			

	<input type="checkbox"/> Yes <input type="checkbox"/> No			
	<input type="checkbox"/> Yes <input type="checkbox"/> No			

SECTION 4: SHARING, SELLING, AND PURCHASING PERSONAL DATA

The Report must include a list of the types of personal data the governmental entity currently shares, sells, or purchases; the legal basis for sharing, selling, or purchasing personal data; and the category of individuals or entities with whom the governmental entity shares personal data, to whom the governmental entity sells personal data, and from whom the governmental entity purchases personal data. (Utah Code § 63A-19-401.3(1)(c), (d), and (e)) Using the check boxes below identify whether, and the types of, personal data the 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, AND PURCHASING
<p>Basic Identification & Contact Information</p> <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	
<p>Demographic & Personal Characteristics</p> <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	

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	
Financial Data <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 • Credit Reports • Credit Scores • Payment History 	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
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	

<p>Education Information</p> <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	
<p>Government Program & Benefits Data</p> <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	
<p>Biometric Data</p> <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	

<p>Online & Digital Identifiers</p> <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"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
<p>Criminal or Legal Information</p> <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	
<p>Vehicle & Property Data</p> <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	

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	
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	
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	
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	

Other :	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
Other :	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	
Other :	<input type="checkbox"/> Share <input type="checkbox"/> Sell <input type="checkbox"/> Purchase <input type="checkbox"/> N/A	

SECTION 5: PERSONAL DATA RECIPIENTS AND SOURCES

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

Mark any categories of individuals or entities with whom personal data is shared, to whom personal data is sold, and from whom personal data is purchased.

PROCESSING ACTIVITY	CATEGORIES OF RECIPIENTS OR SOURCES
Personal Data Shared With:	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities:</p> <ul style="list-style-type: none"> <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 <p>II. International Governmental Entities:</p> <ul style="list-style-type: none"> <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 <p>III. Public Disclosure:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Public Disclosure / Open Records Releases <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors:</p> <ul style="list-style-type: none"> <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 <p>II. Data & Marketing:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Private Sector / Commercial Companies <input type="checkbox"/> Data Brokers / Aggregators <input type="checkbox"/> Social Media Platforms <p>III. Financial & Insurance:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Credit Bureaus or Financial Institutions <input type="checkbox"/> Insurance Providers <p>IV. Healthcare:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Healthcare Providers or Health Information Exchanges <p>V. Media:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Media or News Organizations <p>Research, Education, and Nonprofit Entities</p> <ul style="list-style-type: none"> <input type="checkbox"/> Research Institutions / Universities

<p>Personal Data Sold To:</p>	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities:</p> <ul style="list-style-type: none"> <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 <p>II. International Governmental Entities:</p> <ul style="list-style-type: none"> <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 <p>III. Public Disclosure:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Public Disclosure / Open Records Releases <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors:</p> <ul style="list-style-type: none"> <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 <p>II. Data & Marketing:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Private Sector / Commercial Companies <input type="checkbox"/> Data Brokers / Aggregators <input type="checkbox"/> Social Media Platforms <p>III. Financial & Insurance:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Credit Bureaus or Financial Institutions <input type="checkbox"/> Insurance Providers <p>IV. Healthcare:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Healthcare Providers or Health Information Exchanges <p>V. Media:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Media or News Organizations <p>Research, Education, and Nonprofit Entities</p> <ul style="list-style-type: none"> <input type="checkbox"/> Research Institutions / Universities
--------------------------------------	---

<p>Personal Data Purchased From:</p>	<p>Governmental and Public Sector Entities</p> <p>I. Domestic Governmental Entities:</p> <ul style="list-style-type: none"> <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 <p>II. International Governmental Entities:</p> <ul style="list-style-type: none"> <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 <p>III. Public Disclosure:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Public Disclosure / Open Records Releases <p>Commercial and Private Sector Entities</p> <p>I. Service Providers & Vendors:</p> <ul style="list-style-type: none"> <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 <p>II. Data & Marketing:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Private Sector / Commercial Companies <input type="checkbox"/> Data Brokers / Aggregators <input type="checkbox"/> Social Media Platforms <p>III. Financial & Insurance:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Credit Bureaus or Financial Institutions <input type="checkbox"/> Insurance Providers <p>IV. Healthcare:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Healthcare Providers or Health Information Exchanges <p>V. Media:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Media or News Organizations <p>Research, Education, and Nonprofit Entities</p> <ul style="list-style-type: none"> <input type="checkbox"/> Research Institutions / Universities
---	---

SECTION 6: NON-COMPLIANT PROCESSING ACTIVITIES

The Report must include 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 the GDPR. (Utah Code § 63A-19-401.3(1)(g))

PROCESSING ACTIVITY	STRATEGIES FOR COMPLIANCE

SECTION 7: HIGH-RISK PROCESSING ACTIVITIES

The Report must include a description of the governmental entity's high-risk processing activities. (Utah Code § 63A-19-401.3(1)(b)(iii))

Select all applicable high-risk processing activities the entity engages in and explain why the governmental entity engages in the high-risk processing activity.

☐ Facial recognition technology

Description of Purpose: _____

☐ Automated decision making

Description of Purpose: _____

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

Description of Purpose: _____

☐ Genetic data processing

Description of Purpose: _____

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

Description of Purpose: _____

☐ Geolocation data processing

Description of Purpose: _____

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

SECTION 8: PRIVACY TRAINING COMPLETION

The Report must include the percentage of the governmental entity's employees that have fulfilled the data privacy training requirements described in Utah Code § 63A-19-401.2. (Utah Code § 63A-19-401.3(1)(f))

What percentage of the entity's employees have completed the required data privacy training created by the Office?

Enter %

SECTION 9: CERTIFICATION

I hereby certify that I am the Chief Administrative Officer for the governmental entity named above, and the information provided in this report is accurate to the best of my knowledge.

Name: _____

Signature: _____

Date: _____

Exhibit B

Privacy Policy

Thank you for choosing to be part of our community at Carbon County, Utah ("Carbon," "we," "us," or "our"). We are committed to protecting your personal information and your right to privacy. If you have any questions or concerns about this privacy notice or our practices with regard to your personal information, please contact us at privacy@carbon.utah.gov.

This privacy notice describes how we might use your information if you:

- Visit our website at <http://www.carbon.utah.gov>
- Engage with us in other related ways – including any sales, marketing, or events

In this privacy notice, if we refer to:

- "Website," we are referring to any website of ours that references or links to this policy
- "Services," we are referring to our Website, and other related services, including any sales, marketing, or events

The purpose of this privacy notice is to explain to you in the clearest possible way what information we collect, how we use it, and what rights you have in relation to it. If there are any terms in this privacy notice that you do not agree with, please discontinue use of our Services immediately, and reach out to us with your concerns.

Please read this privacy notice carefully, as it will help you understand what we do with the information that we collect.

TABLE OF CONTENTS

1. [WHAT INFORMATION DO WE COLLECT?](#)
2. [HOW DO WE USE YOUR INFORMATION?](#)
3. [WILL YOUR INFORMATION BE SHARED WITH ANYONE?](#)
4. [WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES](#)
5. [HOW LONG DO WE KEEP YOUR INFORMATION](#)
6. [HOW DO WE KEEP YOUR INFORMATION SAFE?](#)
7. [WHAT ARE YOUR PRIVACY RIGHTS?](#)
8. [CONTROLS FOR DO-NOT-TRACK FEATURES](#)
9. [DO CALIFORNIA RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?](#)
10. [DO WE MAKE UPDATES TO THIS NOTICE?](#)
11. [HOW CAN YOU CONTACT US ABOUT THIS NOTICE?](#)

1. WHAT INFORMATION DO WE COLLECT?

In Short: We collect personal information that 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 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 purchases, such as your payment instrument number (such as a credit card number), and the security code associated with your payment instrument. All payment data is stored by Secure Instant Payments.com. You may find their privacy notice link(s) here: <https://secureinstantpayments.com/sip/client.Instant/privacy.php>.

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

Information automatically collected

In Short: Some information – such as your Internet Protocol (IP) address and/or browser and device characteristics – is collected automatically when you visit our Websites.

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, such as your IP address, browser and device characteristics, operating system, language preferences, referring URLs,

device name, country, location, information about how and when you use our Website and other technical information. This information is primarily needed to maintain the security and operation of our Website, and for our internal analytics and reporting purposes.

The information we collect includes:

- ***Log and Usage Data.*** Log and usage data is service-related, diagnostic, usage and performance information our servers automatically collect when you access or use our Website and which we record in log files. Depending on how you interact with us, this log data may include your IP address, device information, browser type, and settings and information about your activity in the Website (such as the date/time stamps associated with your usage, pages and files viewed, searches and other actions you take such as which features you use), device event information (such as system activity, error reports (sometimes called 'crash dumps') and hardware settings).
- ***Device Data.*** We may collect device data such as information about your computer, phone, tablet, or other device you use to access the Website. Depending on the device used, this device data may include information such as your IP address (or proxy server), device and application identification numbers, location, browser type, hardware model internet service provider and/or mobile carrier, operating system and system configuration information.
- ***Location Data.*** We may collect location data such as information about your device's location, which can be either precise or imprecise. How much information we collect depends on the type and settings of the device you use to access the Website. For example, we may use GPS and other technologies to collect geolocation data that tells us your current location (based on your IP address). You can opt out of allowing us to collect this information either by refusing access to the information or by disabling your location settings on your device. Note however, if you choose to opt out, you may not be able to use certain aspects of the Services.

2. HOW DO WE USE YOUR INFORMATION?

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

We use personal information collected via our 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 enter into or perform a contract with you, with your consent, and/or for compliance with our legal obligations. We indicate the specific processing grounds we rely on next to each purpose listed below.

We use the information we collect or receive:

- **To send administrative information to you.** We may use your personal information to send you product, service, and new feature information and/or information about changes to our terms, conditions, and policies.
- **To protect our Services.** We may use your information as part of our efforts to keep our Website safe and secure (for example, for fraud monitoring and prevention).
- **To enforce our terms, conditions, and policies for business purposes, to comply with legal and regulatory requirements or in connection with our contract.**
- **To respond to legal requests and prevent harm.** If we receive a subpoena or other legal request, we may need to inspect the data we hold to determine how to respond.
- **Fulfill and manage your orders.** We may use your information to fulfill and manage your orders, payments, returns, and exchanges made through the Website.
- **Administer prize draws and competitions.** We may use your information to administer prize draws and competitions when you elect to participate in our competitions.

- **To deliver and facilitate delivery of services to the user.** We may use your information to provide you with the requested service.
- **To respond to user inquiries/offer support to users.** We may use your information to respond to your inquiries and solve any potential issues you might have with the use of our Services.
- **To send you marketing and promotional communications.** We and/or our third-party marketing partners may use the personal information you send to us for our marketing purposes, if this is in accordance with your marketing preferences. For example, when expressing an interest in obtaining information about us or our website, subscribing to marketing or otherwise contacting us, we will collect personal information from you. You can opt-out of our marketing emails at any time (see the "WHAT ARE YOUR PRIVACY RIGHTS?" below).
- **Deliver targeted advertising to you.** We may use your information to develop and display personalized content and advertising (and work with third parties who do so) tailored to your interest and/or location and to measure its effectiveness.
- **For other business purposes.** We may use your information for other business purposes, such as data analysis, identifying usage trends, determining the effectiveness of our promotional campaigns and to evaluate and improve our Website, products, marketing, and your experience. We may use and store this information in aggregated and anonymized form so that it is not associated with individual end users and does not include personal information.

3. 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 your 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 Contract: Where we have entered into a contract with you, we may process your personal information to fulfill the terms of our contract.

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.

More specifically, we may need to process your data or share your personal information in the following situations:

Business Transfers. We may share or transfer your information in

connection with, or during negotiations of, any merger, sale of company assets, financing, or acquisition of all or a portion of our business to another company.

Google Maps platform APIs. We may share your information with certain Google Maps Platform APIs (e.g., Google Maps API, Place API). To find more about Google's Privacy Policy, please refer here <https://policies.google.com/privacy>

4. WHAT IS OUR STANCE ON THIRD-PARTY WEBSITES?

***In Short:** We are not responsible for the safety of any information that you share with third-party providers who advertise, but are not affiliated with, our Website.*

The Website may contain advertisements from third parties that are not affiliated with us and which may link to other websites, online services or mobile applications. We cannot guarantee the safety and privacy of data you provide to any third parties. Any data collected by third parties is not covered by this privacy notice. We are not responsible for the content or privacy and security practices and policies of any third parties, including other websites, services or applications that may be linked to or from the Website. You should review the policies of such third parties and contact them directly to respond to your questions.

5. 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.

We 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 keeping your personal information for longer than 2 years.

When we have 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.

6. 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.

7. WHAT ARE YOUR PRIVACY RIGHTS?

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

If you are a resident in the EEA or UK and you believe we are unlawfully processing your personal information, you also have the right to complain to your local data protection supervisory authority. You can find their contact details here:

https://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm.

8. CONTROLS FOR DO-NOT-TRACK FEATURES?

Most web browsers and some mobile operating systems and mobile applications include a Do-Not-Track ("DNT") feature or setting you can activate to signal your privacy preference not to have data about your online browsing activities monitored and collected. At this stage no uniform technology standard for recognizing and implementing DNT signals has been finalized. As such, we do not currently respond to DNT browser signals or any other mechanism that automatically communicates your choice not to be tracked online. If a standard for online tracking is adopted that we must follow in the future, we will inform you about that practice in a revised version of this privacy notice.

9. DO CALIFORNIA RESIDENTS HAVE SPECIFIC PRIVACY RIGHTS?

In Short: Yes, if you are a resident of California, you are granted specific rights regarding access to your personal information.

California Civil Code Section 1798.83, also known as the "Shine The Light" law, permits our users who are California residents to request and obtain from us, once a year and free of charge, information about categories of personal information (if any) we disclosed to third parties for direct marketing purposes and the names and addresses of all third parties with which we shared personal information in the immediately preceding calendar year. If you are a California resident and would like to make such a request, please submit your request in writing to us using the contact information provided below.

If you are under 18 years of age, reside in California, and have a registered account with the Website, you have the right to request removal of unwanted data that you publicly post on the Website. To request removal of such data, please contact us using the contact information provided below, and include the email address associated with your account and a statement that you reside in California. We will make sure the data is not publicly displayed on the Website, but please be aware that the data may not be completely or comprehensively removed from all our systems (e.g. backups, etc.).

10. DO WE MAKE UPDATES TO THIS NOTICE?

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

We may update this privacy notice from time to time. The updated version will be indicated by an updated "Revised" date and the updated version will be effective as soon as it is accessible. If we make material changes to this privacy notice, we may notify you either by prominently posting a notice of such changes or by directly sending you a notification. We encourage you to review this privacy notice frequently to be informed of how we are protecting your information.

11. HOW CAN YOU CONTACT US ABOUT THIS NOTICE?

If you have questions or comments about this notice, you may email us at privacy@carbon.utah.gov or by post to:

Carbon County

751 East 100 North

Price, UT, 84501

United States

Last Updated: 12/8/21