DRCOG Data Privacy Policy

Table of Contents

Purpose and Scope

The Denver Regional Council of Governments is a planning organization where local governments collaborate to establish guidelines, set policy and allocate funding in the areas of transportation and personal mobility, growth and development, and aging and disability resources.

To make informed decisions, it is necessary for DRCOG to collect, store, analyze, visualize, and report data - some of which may be of a sensitive nature. DRCOG must balance the need for information with the needs of the public, vendors, and partners to maintain the privacy of their personal or proprietary data.

This policy serves as a notice to the public to inform them of our intentions to use data responsibly. It also provides a framework for DRCOG staff to handle protected data by outlining our guiding principles and strategies, although it is not meant to be a procedural implementation guide nor will it cover sensitive information related solely to internal operations.

Guiding Principles

1. **Public trust** - DRCOG prioritizes public trust by responsibly managing and safeguarding personal information collected in support of its mission.
2. **Public good** - DRCOG is responsible for a variety of services and programs that make life better in the Denver region. The data that DRCOG collects is used to support, measure, and evaluate progress toward a variety of shared outcomes and goals.
3. **Responsible governance** - DRCOG develops, maintains, and adheres to policies and procedures that balance the need to protect individual privacy with the need to responsibly use data for public good. DRCOG's governance encourages transparency and accountability.
4. **Responsible stewardship** - DRCOG implements policies and procedures to prioritize privacy and ensure security, including routine reassessments, modifications for continuous improvement, and prompt responsiveness to threats. DRCOG uses best practices and appropriate safeguards to properly secure and protect the integrity of data.

Definitions

- **Data** – information that belongs to DRCOG or for which DRCOG is responsible, including geospatial, tabular, or textual or image information that is maintained in an electronic or physical format.
- **Protected –** Any data that DRCOG is restricted from disclosing, including:
    - **Personally Identifiable Information** (PII)* - information about an individual that could reasonably be used to identify such individual, either alone or when combined with other personal identifying information . PII may include, but not be limited to, first and last name, residence or other physical address, electronic mail address, telephone number, birth date, credit card information, social security number, and some mobility information like specifics of a trip. *DRCOG examples: data submitted to DRCOG to set up an account on our website, respond to a survey, or participate in a program; data supplied to a third-party from which DRCOG gets data (e.g. health or employment information);*
    - **Regulated–** information that is protected by a law or policy. *DRCOG example: Address data provided to DRCOG by the U.S Census is protected by Title 13, U.S Code, and protected health information (PHI) which is protected under the Health Insurance Portability and Accountability Act (HIPAA).*
    - **Proprietary –** information that is protected as privileged under applicable law (e.g., confidential commercial or financial information under the Colorado Open Records Act) or by a contractual

  agreement. *DRCOG example: Employment and housing data provided to DRCOG is protected by a contract with the company that sells the data.*
  - **Confidential –** information that is not protected by any of the aforementioned classifications but that needs protection, as determined by DRCOG. *DRCOG example: contract negotiation status during the RFP process or attorney-client communications.*

- **Public**
  - **Public information –** publicly available data, including unstructured data that is not curated for distribution and may come in a variety of formats. *DRCOG example: meeting materials including attendee contact information.*
  - **Open -** publicly available data structured in a way that enables the data to be fully discoverable and usable by the end users. *DRCOG example: Data available for download on DRCOG.org or the Regional Data Catalog.*

***Exception for Publicly-Available Personal Information**. When DRCOG receives personal information that, in the context it was received, clearly indicates that there is no expectation of privacy, the information is not considered PII under this this policy and this policy does not prohibit its public re-disclosure. An example of this exception would be the re-publication of a publicly-available news article containing personal information or contact information offered to DRCOG on a meeting sign-in sheet.

Roles and Responsibilities

The Data Privacy Policy is governed by these roles and responsibilities:

- **Data Management Committee** (DMC): The DMC is responsible for providing guidance and oversight as it pertains to data policy development and implementation at DRCOG. The DMC is a cross-divisional standing committee made up of representatives from all DRCOG divisions and includes all Data Stewards, the Data Program Manager and the Information Security Officer.
- **Data Program Manager** (DPM): The DPM is responsible for leading the implementation of this policy at DRCOG. The DPM coordinates membership and meetings of the DMC and consults with the Data Stewards in each division. The Data Program Manager is also responsible for maintaining an inventory of protected data and performing audits to ensure its proper handling.
- **Information Security Officer** (ISO): The ISO is responsible for securing and monitoring DRCOG information technology systems and ensuring compliance with DRCOG policies and procedures. The ISO serves as a key advisor to the Data Management Committee.
- **Data Stewards**: Data Stewards are designated by each Division Director. There is one primary and alternate Data Steward per DRCOG division and they are responsible for coordinating efforts pertaining to the implementation of this policy in their respective division. Data Stewards are responsible for maintaining a division-specific inventory regarding protected data unique to their division and providing this to the DPM for inclusion in the agency-wide inventory. The Data Steward fields questions regarding this policy within their divisions and serves as a liaison between division and agency-wide needs.
- **Data Custodians**: Data Custodians are responsible for managing the programs that acquire, produce, store or share data at DRCOG. They are responsible for developing procedures to handle their data that align with this policy and sharing those details with their division's Data Steward.
- **Data Users**: Data Users are all DRCOG staff, stakeholders and partners that use data on behalf of DRCOG.

Classification and Assessment

DRCOG classifies data to determine whether the data is protected or public. If protected, a Privacy Impact Assessment is used to identify and mitigate risks to privacy. Periodically, data may need to be reclassified to ensure adherence to the policy.

Classifying and Reclassifying the Data

A DRCOG Data Steward, in conjunction with Data Custodians, classifies data according to the definitions outlined above. Every effort is made to perform this function prior to obtaining *new* data, to err on the side of caution (i.e. when in doubt, classify) and to adopt the strictest classification applicable while recognizing that as a public entity, DRCOG must comply with the Colorado Open Records Act which favors broad access to public records.

A classification exercise is triggered if any of the following criteria are met:

- Data is being obtained about subject matter with which DRCOG has no prior experience.
- Data is being obtained from a source with whom DRCOG has no prior relationship.
- Data is being purchased.
- Data is, for any reason, suspected to have protected elements.

A classification exercise is not necessary if any of the following criteria are met:

- Data is an update to information that has already undergone classification.
- Data is being obtained from a public source.

The classification exercise includes the following questions, in this order:

- Does the data contain PII (as defined above)?
  - If yes, classify as **PII.**
  - If no, proceed to next question.
- Is the data protected by law?
  - If yes, classify as **Regulated.**
  - If no, proceed to next question.
- Is the data protected as privileged under applicable law or by a contractual agreement?
  - If yes, classify as **Proprietary.**
  - If no, proceed to next question.
- Is the data sensitive for any other reason?
  - If yes, classify as **Confidential.**
  - If no, classify as **Public.**

Reclassification is triggered if:

- A new agreement or contract is signed for the data, requiring a review of terms.
- A data review indicates data needs to be reevaluated because something has changed (e.g. laws, internal systems or platforms, processing workflows, or a security incident).

Performing a Privacy Impact Assessment on Protected Data

If any data is classified as protected, then the DRCOG Data Stewards and Custodians perform a **Privacy Impact Assessment**, which documents the following questions:

- For what **purpose** is the data being obtained?
- What is the **source** of the data? Are there any **alternative** sources?
- In what format and locations will the data be **stored**?

- How will the data be **analyzed**?
- How will results be **reported**?
- How often and by whom will the data be **accessed**?
- With whom, if anyone, will the data be **shared**?
- How will data be **transmitted**?
- How long must the data be **retained**?
- By what method must the data be **destroyed**?
- What is the potential **adverse impact** of unauthorized disclosure?
- If PII, additional questions are asked, such as:
    - Can any action be taken to reduce the amount of PII?
    - Has consent been obtained from and notice given to the affected individual?

The Data Management Committee reviews the classification and assessment and approves implementation steps.

Safeguards

DRCOG employs the following administrative, technical, and physical strategies designed to prevent, detect, and correct any issues pertaining to protected data under our purview.

Staying Informed

- Analyzing and managing potential data security risks by staying abreast of public breaches and emerging industry security practices.
- Continuing to develop policies and training employees about how to safeguard protected data.
- Requiring that employees report potential security incidents to DRCOG supervisors.
- Performing internal, periodic, robust data reviews to ensure protected data is being handled properly.

Minimizing Exposure

- Identifying which employees need to access protected data to perform their duties.
- Limiting employee access to protected data to the minimum amount necessary to perform their duties.
- Implementing procedures for granting, supervising, and terminating employee access to protected data.
- Limiting physical access to electronic data systems (e.g., server rooms).
- Acquiring the least amount of protected data that we require for our use cases.
- Limiting secondary uses of protected data (e.g. conservatively evaluating uses for which the data was not originally obtained).
- Using third-party experts, where appropriate, to handle protected data on our behalf.

Securing Resources

- Requiring visitors to sign in prior to entering DRCOG offices.
- Developing and implementing facility security plans.
- Setting standards for creating, changing, and safeguarding passwords.
- Requiring staff to use data security features like passwords on equipment (e.g., mobile phones, laptop computers, and desktop computers) used for DRCOG purposes.
- Automatically terminating an electronic session (i.e., logging off) after a predetermined time of inactivity.
- Limiting invalid log-in attempts to the DRCOG domain and computers.

Sharing and Transmission

- Carefully evaluating the needs of third-parties to determine if sharing protected data is necessary and if so, entering into contractual agreements that govern the handling of the protected data by the third-party.
- Obscuring protected information prior to sharing using such means as aggregation (e.g. spatial, temporal or demographic summarization) or de-identification (i.e. removal of personal information).
- Working with the Information Security Officer to determine secure options for transmitting protected data, (e.g. encryption, password-protection, or physical media).
- Transmitting protected data in a manner that prevents unauthorized access to the information (e.g., encryption, SSL).
- Considering private those systems that contain both public and private information (e.g. DRCOG's contact relationship management system).

Storage and Retention

- Requiring that physical records containing protected data be marked and placed in a secure location.
- Utilizing encryption systems to protect sensitive information at rest (e.g., database backups) from being accessed or viewed by unauthorized users.
- Maintaining secure information technology infrastructure (e.g. applying patches to operating systems, firewalls, and anti-malware software).
- Implementing procedures governing the destruction or removal of protected data in accordance with DRCOG's Record Retention Schedule.

Remediation

- Remediating breaches according to applicable State and federal laws, contractual requirements or other guidelines that apply (e.g. analyzing root cause(s), notifying affected parties, consulting with legal advisors, and implementing corrective measures).

Exclusions

Sensitive data used for internal operations (e.g. infrastructure passwords, HR records) which do not endanger public trust and are governed by other established policies that need not be reiterated verbatim (e.g. State HR Law, DRCOG Computer Security Policy) are excluded from this policy.

Legal

Law and Regulatory Compliance

DRCOG shall abide by all requirements of C.R.S. § 24-73-101, *et seq*.

DRCOG shall evaluate data on a case-by-case basis to determine if personal identifiable information may be used to identify and individual including, but not limited to a combination of two or more of the following identifiers: first and last name, residence or other physical address, electronic mail address, telephone number, birth date, place of birth, credit card information, or social security number. DRCOG may release PII and other data if required by law, including but not limited to the Colorado Open Records Act (CORA).

DRCOG shall abide by all State and Federal data and privacy laws, including but not limited to the Colorado Open Records Act (CORA) and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Notices to the Public

In the event of a security breach or suspected security breach, an investigation will ensue to determine the likelihood that personal information has been or will be misused. Notice to affected parties shall occur in the most expedient time possible, and no later than thirty days after the date of a suspected security breach. All notices will be made in accordance with C.R.S. § 24-73-103 and/or HIPAA. In the event of a security breach affecting five hundred or more Colorado residents, the Colorado Attorney General will be notified.

Consent

DRCOG typically only collects PII from an individual who has voluntarily provided that information to DRCOG. Only the minimum amount of PII necessary to fulfill the task or objective will be collected. Such information will not be used for other purposes without the consent of the individual. Persons providing their PII to DRCOG should carefully read program-specific privacy policies to better understand how their information may be used. When obtaining data from a third-party, DRCOG will confirm that data has been originally obtained in an appropriate way.

References

City and County of Denver Executive Order No. 143: Protected Data Privacy Policy	https://www.denvergov.org/content/dam/denvergov/Portals/executiveorders/143-Protected_Data_Privacy_Policy.pdf
City of Aurora Information Technology Department Data Privacy Policy *DRAFT*	N/A
City of Boulder Data Policy *DRAFT*	N/A
City of Los Angeles Information Technology Guidelines for Handling of Data from Mobility Service Providers	https://ladot.lacity.org/sites/default/files/documents/ladotguidelinesforhandlingofdatafrommsps2018-10-25.pdf
LADOT Data Protection Principles	https://ladot.io/wp-content/uploads/2019/03/LADOT_Data_Protection_Principles-1.pdf
NACTO Policy 2019: Managing Mobility Data	https://nacto.org/wp-content/uploads/2019/05/NACTO_IMLA_Managing-Mobility-Data.pdf
SANDAG Privacy Policy for Collection, Management, and Storage of Personal Information	https://www.sandag.org/uploads/publicationid/publicationid_1962_19334.pdf
Smart Columbus Data Privacy Plan	https://d3hzplpmmz6qe4.cloudfront.net/2019-07/Smart%20Columbus%20Operating%20System%20Data%20Privacy%20Plan_0.pdf

Version History

Version 1.1 – August 2020

Appendix A: Examples of Use

DRCOG continually evaluates new data products that could inform our work. The following list illustrates examples of data in use at DRCOG at the time of writing.

Facilitation and Communication

DRCOG facilitates meetings and events during which certain **contact information** may be collected. Additionally, DRCOG maintains contact information for the purpose of informing and engaging our partners, peers, elected officials, local government representatives and other similar stakeholders.

Data can include name, email, organization, social handle, phone number and related contact information. Often this contact information is not available elsewhere publicly. Examples include:

1. Meeting attendance records
2. Customer relationship management (CRM) system
3. Campaign Monitor system

Online Engagement

DRCOG engages the public through its web properties and may collect certain **user information**.

Data can include contact information, usernames, passwords, and related profile information that is submitted to DRCOG via our web properties. Examples include:

- Web accounts
- Event registrations (BTWD, Citizen’s Academy)
- Award nominations (WTG, MV, JVC)
- Social pinpoint (online engagement tool)

Program Administration

DRCOG administers various programs which require collecting **participant information** and **project information.**

Data can include contact information as well as behaviors, preferences, needs, contributions, locations, associated organizations and related identifiers. Examples include:

- Location/route/travel information (e.g. My Way to Go, Schoolpool, Front Range Travel Counts, Commercial Vehicle Survey)
- Initiative partners/sponsors (e.g. Gotober, Annual Awards)
- Employer information (e.g. Guaranteed Ride Home)
- Medical information (e.g. Accountable Health Communities, Ride Alliance)
- Intake forms, case notes (AAA programs like Veterans, Transitions)
- Business contact information (e.g. Way to Go)
- Survey responses
- Photos and audio/visual recordings
- Comments (Youth advisory committee, public comments at hearings, online comment maps for Vision Zero, Freight, TIP, Land Use Forecast)
- Disability status; destination (Ride Alliance Project)

Data can also include information on specific projects. Examples include:

- TIP applications, budgets, designs
- Traffic signal projects
- Sensitive infrastructure (fiber)

Modeling

DRCOG develops and maintains a series of models that forecast land use, transportation, and air quality.

Data can include building permits, trip routes, travel behavior, and related information. Some data are sourced through a third-party and governed by specific agreements. Other data is created in-house and only distributed in final form at DRCOG's discretion. Examples include:

- Building permits from Construction Monitor (Land Use Block Model)
- Travel behavior from INRIX (Focus Travel Model)
- FOCUS model and supporting data
- Land use block model and supporting data
- Streetlight data (Focus Travel Model)

Plan Development and Evaluation

DRCOG uses a variety of data sources to develop regional plans and to monitor progress towards both regionally-set and federally-mandated goals.

Data can include employment, housing, travel behavior and demographics. Examples include:

- Employment from Infogroup and QCEW (Metro Vision Metrics)
- Housing from Costar (Metro Vision metrics)
- Bike and scooter trips from various providers (Active Transportation Plan)
- Crash data (Vision Zero)
- Unsafe facilities (Vision Zero)

Member/Partner Support

DRCOG supports members and partners by providing access to restricted datasets that are sourced from third-parties and governed by specific agreements. DRCOG also uses restricted datasets to help members participate in federal programs.

Data can include employment data, address data and imagery. Examples include:

- Nearmap streaming imagery subscription
- DRAPP imagery (current year)
- Census addresses (for the LUCA program)