CITY OF SEATTLE MOBILITY DATA

Privacy and Handling Guidelines

Last updated: December 30, 2019

The City of Seattle, through its Department of Transportation (SDOT), works to deliver a transportation system that provides safe and affordable access to places and opportunities. This is reflected in the work SDOT does to manage the public right-of-way, ensure safe movement of people and goods, and improve infrastructure and mobility choices throughout the city. As SDOT works to advance our core values of equity, safety, mobility, sustainability, livability, and excellence, we collect data necessary for performing our work while protecting against the misuse of personal mobility data.

As part of its free-floating bike share permit, SDOT requires bike share vendors (Operators) operating on Seattle's right-of-way to comply with the Mobility Data Specification (MDS). This specification organizes the vehicle and trip data minimally necessary for SDOT to monitor data compliance in accordance with permit rules. MDS sets a consistent standard for sharing vehicle status data, e.g. whether a vehicle is in use or parked (via a Status Changes feed), and trip data, e.g. indicating location and length of trip (via a Trips feed), from Operators to cities. While MDS was created by Los Angeles Department Of Transportation, governance of the specification has transferred to the newly formed Open Mobility Foundation, an open-sourced non-profit foundation governed by cities with participation by the private sector and other non-governmental entities.

Though the vehicle and trip data SDOT collects from Operators does not contain personal information associated with an individual, SDOT applies the City of Seattle Privacy Principles and Information Security Data Classification Guidelines for collecting, transmitting, storing, and using personal information in addition to the following data protection standards. SDOT recognizes that there are inherent privacy risks associated with collection of trip location data, which, when combined with other publicly-available data, can be used to identify individuals making the trips. However, some SDOT trip location data collection is necessary for program evaluation and general city planning purposes, such as establishing baselines for emerging and untested mobility services operating in the public right-of-way.

The following data protection standards apply to all data obtained from Operators to carry out the City of Seattle's and SDOT's data protection responsibilities:

1. **Transparency and Accountability (How we use trip information):** The public should receive a clear description of the data used by SDOT and the ways such data is pertinent to the responsibility of protecting the public right-of-way.
    a. The City of Seattle and SDOT encourage Operators as defined in MDS to inform their customers that vehicle data is being shared with the City of Seattle. (Current user terms for active Operators here: Jump, Lime)
    b. The City of Seattle voluntarily shares certain information with the public to increase transparency, accountability, and customer service and to empower companies, individuals, and non-profit organizations with the ability to harness a vast array of useful information to improve life in our city.
    c. To the extent permitted by law, any tool that is commissioned to be built or licensed for use by the City of Seattle and used in conjunction with the MDS shall be designed to comply with these guidelines.
    d. SDOT will publish a list of the data types collected via MDS and the length of time that data is retained.

City of Seattle

2. **Data Categorization and Security:** SDOT classifies trip data as Sensitive, following the Information Security Data Classification Guidelines. Based on this determination, city-approved access and security controls are applied to the data. Seattle's formal information security program and comprehensive set of security controls are grounded in the City of Seattle's Information System and Security Policy (ISSP). The principles established by the ISSP govern this data and all other City data, including but not limited to incident and emergency response reporting.

3. **Data Minimization (Collecting and keeping only what we need):** We only collect information required to deliver and manage City services and programs, and keep it as long as legally required. The City of Seattle and SDOT will collect, access, use, store, process, transmit, dispose of, and disclose data in accordance with the City of Seattle's previously mentioned Security Policy, ISSP. Seattle will monitor and adopt industry best practices for aggregation and obfuscation of trip data (see some methods below), evolving over time as new best practices and strategies emerge.
    a. To the extent that data is used to help us make transportation policy and planning decisions, it will be stored until its administrative purpose is served, or as required by applicable records retention schedules and in accordance with the City of Seattle Data Classification Guidelines.
    b. SDOT is not currently accessing real-time data. Queries run on a daily refresh schedule, not intermittently throughout the day.
    c. SDOT does not currently store detailed route records from the Trips feed; rather, we store only trip origin and trip destination data.
    d. SDOT currently stores trip origin and destination geolocation coordinates to four decimal places (i.e., accurate only to 25-30 feet).
    e. SDOT commits to exploring pre-processing aggregation methods (e.g., aggregating trips to fifteen-minute increments) to group and store information that would further obfuscate individualized trip data.

4. **Data Sharing and Access Limitations:** SDOT only allows access to data by authorized persons or as required by law. When proactively making the data public, SDOT will work to ensure that reidentification risks are minimized.
    a. Law enforcement and other government agencies, whether local, state, or federal, will not have access to raw trip data other than as required by law, such as a court order, subpoena, Public Records Request, or other legal process.
    b SDOT and the IT Department limit internal access to pre-approved staff who have been trained on the appropriate use and handling of this data to ensure compliance with privacy and security requirements.
    c. When voluntarily sharing or publishing raw data (i.e., when not otherwise legally required to release data), SDOT prohibits any third-party access or use of raw data for third-party purposes. The City of Seattle does not sell or in any other way monetize the data. The City of Seattle only allows third parties to access raw data if they are under City contracts that limit the use of the raw data to purposes directed by SDOT and as needed for SDOT's operational and regulatory needs.
    d. If the City of Seattle makes a determination that it is appropriate to voluntarily make data public (such as via the City of Seattle's Open Data Portal and after completing a privacy review), and to the extent permitted by law, SDOT will release the data aggregated, blurred or otherwise obfuscated such that reidentification risk is minimized.

The City of Seattle and SDOT reserve the right to amend this data handling policy at any time.