


CITY OF LOS ANGELES
INTER-DEPARTMENTAL CORRESPONDENCE

Date: June 14, 2020

To: Honorable City Council
c/o City Clerk, Room 395
Attention: Honorable Mike Bonin, Chair, Transportation Committee

From: Seleta J. Reynolds, General Manager 
Department of Transportation

Subject: **Data Protection Principles/Use and Retention (CF #19-1355)**

SUMMARY

The Los Angeles Department of Transportation (LADOT) published Data Protection Principles (Principles) to manage and protect mobility data required by its dockless mobility permits in April, 2019. The Los Angeles City Council (Council) directed LADOT to incorporate these Principles into all business lines that use the Mobility Data Specification (MDS), to report back on the specific regulatory purposes for the receipt and use of each type of data required by MDS, and to develop data retention and minimization policies that determine the length of time each type of data is retained. The following report responds to that direction.

RECOMMENDATIONS

The City Council RECEIVE and FILE this report.

BACKGROUND

In 2018, after private companies deployed dockless scooter and e-bikes on City of Los Angeles Streets, Council created Dockless Shared Mobility Pilot rules and guidelines to permit and regulate dockless services operating in the public right of way. These rules and guidelines include a standard data sharing requirement for all permitted Mobility Service Providers (Providers). The Mobility Data Specification (MDS) is a standard that allows for direct data exchange with companies without getting information directly from or about their customers. It allows the Department to more efficiently and effectively fulfill its regulatory and operational responsibilities while bringing dockless mobility to scale and ensuring better transportation services for residents and commuters. In the City of Los Angeles, this tool allowed LADOT to permit nearly 40,000 devices, confirm deployment in disadvantaged and underserved communities, and ensure compliance with regulations that reduce sidewalk clutter and oversaturation and prohibit riding in protected areas.

Regulatory and operational data received throughout each service day includes vehicle specific identification, stationary vehicle location, vehicle unlock/lock and vehicle status change with reason, including when a vehicle enters or leaves service. LADOT receives vehicle route data that informs planning and infrastructure decisions at a 24-hour delay. Using MDS, LADOT requires Providers to supply data via an application programming interface (API) and abide by a Service Level Agreement (SLA), which

details technical requirements for MDS compliance. This sets a consistent standard for the transfer, use, and protection of vehicle data from Providers to LADOT.

Throughout the Dockless Shared Mobility Pilot program, this data allowed LADOT to audit the compliance of operators, and confirm the accuracy and validity of the data they provided. With this data, LADOT is able to enforce a set of specific regulatory use cases, and inform planning and investment decisions with a high level of confidence that the data accurately expresses what is happening on the public right of way. Without the ability to independently audit and verify private Provider's activities in the public right of way, other compliance and planning actions are subject to question.

As private companies continue to develop and deploy tech-enabled modes of transportation that rely on the public right of way for profit, LADOT and other regulating agencies will require digital tools to adequately protect public interest while allowing innovative mobility to scale and prioritizing the protection of individual privacy. LADOT recognizes the inherent sensitivity of mobility data. In response to private sector input and feedback from privacy focused non-profit organizations, LADOT developed its Data Protection Principles (Attachment A), that outline standards for classifying, handling, and sharing mobility data to ensure we appropriately protect mobility data provided in compliance with MDS. These principles ensure that we keep mobility data confidential. The data is not subject to public records requests and cannot be accessed by law enforcement without legal process. These Principles limit third party access and establish a Master Data License and Protection to govern any third party sharing. They also commit the Department to data handling security measures and publicly available transparency reports.

In November 2019, City Council directed LADOT to incorporate the Principles into all applicable rules and guidelines for programs that use MDS and to provide a report detailing specific regulatory purposes for the receipt and use of each type of data required by MDS along with an enhanced data retention and minimization policy that determines the scope of time each type of data is retained.

DISCUSSION

The Department now uses MDS to manage shared bikes and scooters. LADOT is compliant with existing City guidelines on data protection and handling, but is adding specificity to adapt and improve its policies and practices to manage new data sets built through MDS and address important data privacy needs.

City of Los Angeles Guidelines for Data Protection

In 2016, the Information Technology Policy Committee (ITPC) adopted the Information Classification Policy and Information Handling Guidelines (Attachment B) which detailed the City's approach to different classifications of data including public information, open data, internal information, confidential information, and restricted information. These guidelines include definitions and steps to storing, labeling, and sharing different classifications of records. In addition to ITPC's guidance, the City of Los Angeles documents extensive and comprehensive Records Retention Policies in Division 12 of the Administrative Code.¹ LADOT's existing data handling and retention practices are compliant with Citywide guidelines and the Administrative Code. The Data Protection Principles provide additional

¹ City of Los Angeles Administrative Code, Division 12.

http://ens.lacity.org/clk/rmdroot/clkrmroot108519564_05112004.pdf

specificity to current regulation to directly apply to MDS as well as other data sets the Department holds.

LADOT manages 50 business lines ranging from providing transit service to permitting for-hire companies to mitigating traffic impacts through policy. Several programs require the use or collection of data, including information such as driver's licenses, home addresses, credit card information, criminal records used for background checks, age, income, company financial records, crash information, traffic volume surveys, and video feeds. LADOT stores information in a variety of formats and systems, including digital formats and hard copies, and receives data through periodic reports, API feeds, or sharing with other agencies and organizations. LADOT classifies many of these data sets as confidential; does not share personally identifiable and confidential information; and destroys data when it is no longer needed or when the period for required retention has passed.

Incorporating Data Protection Principles into Programs

LADOT recognizes the sensitivity of trip location data received from MDS, and the potential risks there could be to derive personally identifiable information if it is combined with other sources of rider data. MDS is unable to capture any directly personal identifiable information from riders; however, to address potential risks, the Department classifies mobility data as confidential. The Department released a draft set of data protection principles, accepted public comment and published a revised and final version of the Principles in April 2019 along with all public comment received. The Principles document adds further protection on top of the existing Citywide data protection guidelines and regulations and applies to all data received from permitted shared mobility Providers. For example, the principles specify that LADOT will not release the data to law enforcement absent a legal process. These Principles establish a consistent standard for LADOT's approach to individual privacy, which include data categorization, data minimization, access limitation, prohibition of data monetization, security, and transparency.

As detailed in the Principles document, LADOT designates raw (not aggregated) trip data as Confidential Information, and withholds this Confidential Information as exempt from release under the California Public Records Act. LADOT requires data minimization and limits access to raw trip data related to vehicles and vehicle trips solely to that which is required for LADOT's operational and regulatory needs as established by the City Council. As part of its evolving data protection practices, LADOT will continue to enact appropriate administrative, physical, and technical safeguards to properly secure and assure the integrity of data.

In April 2019, LADOT developed a Master Data License and Protection agreement required for any third party requesting access to trip data in the course of providing services to LADOT (Attachment C). The agreement strictly limits how outside parties can use the data and how those third parties must protect the data. LADOT requires any third party entity to sign the Master Data License and Protection before sharing any disaggregate data. Similarly, for internal city requests for data other than law enforcement (which can only access the data through a legal process), LADOT requires a Memorandum of Agreement that enacts similar protections and requirements to the Master Data License Agreement. LADOT will work with the City Attorney to continuously review the Master Data License and Protection Agreement to ensure it is suitable for third party entities.

In March 2020, LADOT updated its Rules and Guidelines for the dockless mobility program (Attachment D) to reflect the Principles. As future programs look to incorporate MDS, LADOT will update corresponding program rules and guidelines accordingly, including car sharing permit requirements and

the new for-hire permitting program launching later this year. LADOT will also require MDS integration and apply the Principles to new programs such as Mobility Hubs.

MDS Transparency Report

LADOT has received 17 external requests for mobility data since the launch of the dockless permit program. The attached transparency report details these requests (Attachment E), which include requests for scooter trip origins and lengths, deployment activity, high activity corridors, and 311 service requests. LADOT classifies individual trip data as confidential, does not share or publish disaggregated data with other entities, including other government entities, and has denied all requests for individual dockless trip or deployment data. Data provided to third parties not governed by the Master Data License and Protection agreement is limited to aggregate data for high level statistical analyses such as those previously reported to City Council.

As of this publication, the following five companies have either signed the Data Licensing and Protection agreement or used MDS data in the course of their work pursuant to the Standard Provisions for City Contracts: BlueSystems, Ellis & Associates, Nelson Nyaard, Toole Design, and Remix. LADOT also requires that any City Departments requesting access to data to sign a Memorandum of Agreement that stipulates the same requirements per storage, handling, and security as the Master Data License Agreement. LADOT will not grant access to disaggregate mobility data to law enforcement and other government agencies except when required by law, such as a court order, subpoena, or other legal process.

LADOT is testing ways to publish de-identified² data sets from MDS APIs to share valuable insights with the public through the City’s open data portal without compromising the privacy of riders upon conclusion of the pilot underway through September 2020.

Data Collection for Regulatory Compliance

To regulate the Dockless Shared Mobility Program, LADOT requires information from companies about their dockless mobility devices that are in the public right of way. LADOT receives the following data points from permitted Providers at the respective time intervals:

Table 1: MDS Data Types Collected

Data Type	Time Interval	Description / Purpose
Vehicle Identification Number and Associated Information	Within 5 seconds of an event	Allows LADOT to assign an action / behavior to a unique vehicle and corresponding Provider. This information also includes propulsion type, vehicle type, and manufacturing year.

² De-Identification is a general term for any process that removes the association between a set of identifying data and the data subject. Source: Garfinkel, Simon L. “De-Identifying Government Datasets”, NIST Special Publication 800-188 (2nd Draft) Page vii.

Vehicle Location	Within 5 seconds for Unlock / Lock and 24 hours for location during a trip.	Allows LADOT to locate the vehicles with latitude and longitude. This is essential for physically locating vehicles and for measuring regulatory compliance against MDS policy.
Vehicle Unlock / Lock	Within 5 seconds	Allows LADOT to know where and when a Provider releases a vehicle to a rider or returns a vehicle to their control. LADOT is also able to determine trip duration using these data types.
Vehicle Status and and Change Reason	Within 5 seconds of the vehicle status change (in-service, out-of-service etc)	Allows LADOT to differentiate between user activity and Provider activity related to a vehicle. This includes provider deployment, user vehicle lock, removal for maintenance, vehicle battery charge level, and is essential to assigning responsibility.
Trip Route	Within 24 hours after the trip concludes	Allows LADOT to understand the route that a vehicle took in order to inform planning.
Trip Cost (Optional Field)	Historical data, within 48 hours after the trip concludes	This data point is optional and provides insight into trip costs to support planning and policy decisions.
Parking Verification (Optional Field)	Historical data, within 48 hours after the trip concludes	Allows Providers to share an image of vehicles in order to verify compliance and assess 311 service requests.

LADOT uses this data to fulfill a number of regulatory compliance use cases designed to mitigate negative impacts and protect public interest while providing equitable mobility options. The Department receives a minimum amount of dockless mobility data to uphold its responsibility to enforce regulatory compliance with the City's adopted requirements in the program rules and guidelines. MDS provides historic data to inform policy and planning and achieve the City's key mobility goals.

Regulatory use cases that require individual device-specific data throughout the day include:

- Verifying Provider data reporting accuracy, completeness, and compliance with LADOT SLA
- Monitoring oversaturation of Provider vehicle density, fleet caps, and sidewalk clutter
- Monitoring vehicle deployment compliance throughout the city, including in disadvantaged communities and special operations zones
- Enforcing geofence restrictions (e.g. no riding on Venice boardwalk)
- Auditing vehicles for operational compliance, safety, and functionality
- Managing and implementing special event restrictions
- Responding to emergency events
- Managing and verifying 311 complaint responses by Providers
- Reviewing and verifying device removal from right of way due to safety violations
- Ensuring and verifying status and number of unsafe or broken vehicles

Planning and policy use cases informed by aggregated device data and route data provided at a 24-hour delay include:

- Infrastructure investment allocations
- Parking infrastructure deployment
- Development and management of equity zones
- Oversaturation analysis
- Development of open data sets

Table 2: Data Use Cases

Use Case Name	Use Case Type	Data Used	Description
Ground Truth	Compliance	Vehicle ID, Vehicle Unlock, VehicleLock, Vehicle Status, Vehicle Location	All other use cases and compliance rely on the ability of LADOT to independently audit, verify, and trust that the data received from Providers is accurate, complete, and in accordance with the LADOT SLA. Requiring notifications to be sent within seconds of the permitted Providers’ activity on the public right of way makes it possible both for LADOT to physically verify ground truth and difficult for Providers to manipulate the data prior to sending. The combination of visible vehicle ID, status, and location allows for critical field validation with the MDS mobile audit software application.
Vehicle Caps	Compliance	Vehicle ID, Vehicle Unlock, Vehicle Lock, Vehicle Status, Vehicle Location	These data sets allow LADOT to monitor how many and where Providers deploy vehicles, to enforce permitted vehicle caps that ensure program compliance, avoid oversaturation, and encourage equitable distribution Effectively measuring tens of thousands of scooters is only possible with accurate record of vehicle ID, status, and location.
Fire / Evacuation	Compliance / Safety	Vehicle ID, Vehicle Unlock, Vehicle Lock, Vehicle Status, Vehicle Location	These data types allow LADOT to hold Providers accountable for compliance to emergency policies issued by LADOT. Accurate vehicle location status also provides City staff an accurate view of activity and scooter usage in affected areas.
Infrastructure Investment	Planning / Capital Investment	Vehicle Unlock, Vehicle Lock, Trip Route	LADOT uses these data types to develop a trusted and aggregated view of trip routes to drive policy decisions, without exposing individual trips. We validate and aggregate all trip route data received for this use.
Open Data Set	Transparency / Public Stewardship	To be determined, but may include: Vehicle Unlock, VehicleLock, Trip Route, Trip Duration, Vehicle Status, Vehicle Location	All data types may assemble aggregated and anonymized data sets available for publication.

Data Privacy: Minimization, Anonymization and Retention

The City is not new to data privacy techniques and sound practices. Applying data privacy treatment practices to MDS requires close coordination with the City Attorney and ITA, consultation with community groups, the public, other cities, and industry experts.

Twenty-seven cities and governmental agencies in the US and over 80 internationally currently use MDS, which is maintained by the global non-profit Open Mobility Foundation (OMF). Through OMF, LADOT engaged with peer cities to learn how they applied municipal data privacy policies to support MDS. LADOT explored data handling and management practices in Boston, MA; New York City, NY; Kansas City, MO; Louisville, KY; Minneapolis, MN; and Seattle, WA, to identify benchmarks on existing data retention policies throughout the country. In addition, LADOT consulted with data privacy experts to identify methodologies and strategies consistent with other government entities while meeting data privacy standards shared across multiple industries.

As directed by Council, LADOT continues to incorporate best practices from these cities into updated Data Protection Principles to improve. This update will provide clarity on the operational steps LADOT will use to protect data the Department receives, among its various work programs including MDS. Prior to publication, LADOT will work closely with the City Attorney and ITA to ensure it meets all legal and regulatory requirements both at the City and State level.

Data De-Identification and Treatment Methodologies

Data privacy methods are specific to their regulatory purpose. Therefore, the treatments and methodologies to de-identify data must center around the use cases discussed above. For each use case, LADOT has identified specific data treatments or strategies as follows:

Data Minimization Approaches:

MDS Metrics and Aggregation: LADOT stores some data in aggregate form for measures such as vehicle counts by status, trip counts, active vehicle counts, and public right of way use. The notifications are grouped by time intervals and geographic areas such as City Council District, census tract, traffic analysis zone, or other geospatial regions. The MDS metrics allow LADOT to analyze program impact trends, Provider vehicle cap compliance, or needs for future transportation planning.

Trip Origin/Destination Binning: Trip origin and destination are particularly important data for planning and regulatory use cases but also represent more sensitive mobility data that becomes less sensitive over time. Trip binning involves rounding trip starts and ends to hourly time intervals and grouping them by geospatial zones such as City Council District, census tract, traffic analysis zone, or spatial indexing system (s2³ or h3⁴). LADOT uses origin/destination data to assess trip volumes by region and time of day.

³ <https://s2geometry.io/>

⁴ <https://eng.uber.com/h3/>

Trip Segment: A trip segment is the association of a vehicle trip with a GPS path that is then grouped by street segments the vehicle traversed. Street segments are then associated with Los Angeles city centerlines and used to aggregate the number of trips by time, direction of travel, and most traveled street segments. LADOT uses trip segment data to analyze traffic patterns and turning movements on street segments, by time of day. This data is particularly useful in measuring effectiveness of infrastructure investments (e.g. new bike lanes) and assessing long range transportation planning efforts or investments.

Data Treatments:

Encryption: LADOT currently encrypts all data notifications it receives through MDS both in transit and at rest using the AES-256 algorithm, an advanced encryption standard for electronic data based on specifications set by the U.S. National Institute of Standards and Technology.⁵ LADOT reserves the right to change its encryption methods if they are found to be vulnerable to attack.

K-anonymization: All of the above minimization approaches (MDS metrics, origin/destination binning, and trip flows) support k-anonymization.⁶ This approach guarantees that no fewer than a specific number of trips can be uniquely grouped to a given time period and spatial zone. For example, LADOT can set “k” to 10 minimum trips per census tract per week, so if fewer than 10 trips occurred within a given census tract that week, the data set would not contain the location of any trips for that tract for that week and would instead be counted only at the city district grouping for that week. The time and geography groupings used in k-anonymization can be adjusted to achieve an optimal binning strategy, whereby if the k value is not met then a larger spatial bin is used while still retaining the defined k-anonymity property. In the example, while a census tract may experience the minimum number of trips to appear in the data set, those trips could still be included in the total for the entire City Council District.

Differential Privacy: In addition to and extending the above approaches, LADOT is exploring the feasibility and value of applying a variety of differential privacy techniques with additive noise mechanisms.⁷

As LADOT continues to receive mobility data through MDS, the Department will use a combination of these data treatments and strategies for each data use case. No use case will leverage a single de-identification, minimization, or anonymization treatment, but a combination of those listed above, as well as other future treatments as tools to protect data privacy evolve over time. LADOT will stress test a combination of de-identification treatments in a secure data testing environment to assess their effectiveness and characterize the vulnerabilities and risks the data.

Data Retention

To protect individual privacy, MDS is governed by more stringent retention policies than existing datasets maintained by the City. Peer cities and experts agree that data should only be retained for as

⁵ https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

⁶ <https://en.wikipedia.org/wiki/K-anonymity>

⁷ https://en.wikipedia.org/wiki/Differential_privacy

long as it is necessary for the data's intended purpose and use. LADOT assessed each required data's purpose and use to ensure we appropriately retain or delete data. For retained data, LADOT set specific timelines for use, and the data will be deleted once the retention period expires, as advised by City Attorney or dictated by California State Law.

Similar to privacy-preserving data strategies, data retention periods are highly specific and are determined by the purpose for data collection, intended use, and approved purposes if the data is shared outside LADOT. In conference with City Attorney, data privacy experts, internal research, and discussions with peer cities, LADOT identified the following retention policies, which are in compliance with the City Administrative Code Section 12.3(b), and subject to input from ITA and the City Attorney going forward:

- Depending on its purpose and role in future adjudication, any location data LADOT receives will be deleted, or de-identified to eliminate re-identification, within 30-90 days from the time of receipt or collection.
 - Location data will be deleted or de-identified within 30 days of receipt or collection for Safety and Planning/Capital Investment Use Case Types.
 - Location data will be deleted or de-identified within 90 days of receipt or collection for Compliance Use Case Types.
- LADOT will place the de-identified data in cold storage and evaluate every 2 years to determine if the Department should retain the data and if it remains sufficiently de-identified as defined by the City Attorney and/or California state law.

Data and Equity

As part of its evaluation of the Dockless Shared Mobility program, LADOT and a team of consultants convened a Core Advisory Board (CAB) (Table 3) and engaged with experts and stakeholders to analyze equity considerations for the Dockless program, including equitable approaches to data. The CAB was comprised of nonprofit leaders and provided feedback to LADOT on Dockless mobility challenges, government-mandated mobility data, and ways to incorporate equity into the department's approach to both. This team worked closely with LADOT staff and leadership, and engaged with community leaders, advocates, and equity experts.

Table 3: Core Advisory Board Composition

Organization / Affiliation	CAB Member
AARP	Stephanie Ramirez
Natural Resources Defense Council	Damon Nagami
Pacoima Beautiful	Veronica Padilla
Prevention Institute	Manal Aboelata
Southern California Resource Services for Independent Living (SRCS-IL)	Hector Ochoa

South Los Angeles Transit Empowerment Zone (Slate-Z)	Effie Turnbull Sanders*
Vera Institute of Justice	Stacey Strongarone**

*Ms Strongarone was only able to attend one meeting.

**Ms. Turnbull Sanders was not able to attend any meetings and left the CAB due to scheduling conflicts

In addition to developing guiding equity principles for the future of the Dockless Program and all other Department programs and services, the consultant team identified several priority considerations LADOT will use to inform future steps for handling data. Stakeholders stated LADOT’s past communications centered on agency goals, rather than issues of public interest, did not sufficiently articulate public benefits derived from MDS data. Interviewees and CAB members also expressed the Department still needs to build trust to engage with historically oppressed and disenfranchised communities, and noted Dockless program data is not publicly accessible. Additionally, LADOT identified data aggregation methods as a key component to providing equitable access to shared mobility. Aggregated data could mask inequalities and impacts, and the Department will integrate equity goals and principles when determining minimization methods for analysis and for communicating MDS data.

The team recommended LADOT provide further education around MDS through community engagement and integrate community concerns into the architecture of the data specification itself. This includes providing explanations of how LADOT is using Dockless mobility data to solve problems and address community impacts, and identifying data points to include in the API that will inform equity metrics. Additionally, the consultant team proposes the Department be more transparent about risks associated with receipt of large amounts of mobility data, and create feedback loops and advisory groups to keep the community engaged in LADOT’s data management process. Lastly, they recommend publishing data sets derived from MDS, allowing stakeholders to hold LADOT accountable for how it handles mobility data, as well as for how the Department uses it to drive decisions.

LADOT Data Principles Update

LADOT plans to consolidate current existing policies and publish a singular guiding document updating the existing Principles to inform how LADOT can further protect all the data it collects - not only dockless vehicle data. The following features are part of that update:

- Expand upon the Data Privacy Principles document to include a formal, sustainable privacy and data management process with specific data handling guidelines for use cases.
- Publish regular transparency reports that will be made available to the public.
- Include an accounting of potential risks associated with collecting and sharing data as part of a transparency report.
- Re-assign the transparency reporting function to LADOT’s Administration and Field Operations Group.
- Continue staff training on privacy principles and policies established as part of this program.
- Publish aggregated MDS data sets to the City’s Open Data Portal in September 2020 to promote transparency.
- Research, evaluate and test new and different strategies and techniques as they evolve over time and stress test the strategies and techniques in a secure data testing environment prior to publishing MDS data on the Open Data Portal.

- Integrate equity goals and principles when determining minimization methods for analysis and for communicating MDS data.
- Work with community organizations to balance individual mobility data privacy with accessible anonymized mobility data sets for the public to be able to better understand and analyze their own communities.

LADOT will continue to identify new protocols to guide the Department in handling data, and define procedures for data minimization, anonymization, and retention, which will be revisited on an annual basis. New findings will be published in future Transparency Reports.

FISCAL IMPACT

There is no fiscal impact as this report is informational.

SJR:MP:js

CITY OF LOS ANGELES

CALIFORNIA

Attachment A

Seleta J. Reynolds
GENERAL MANAGER



ERIC GARCETTI
MAYOR

DEPARTMENT OF TRANSPORTATION
100 South Main Street, 10th Floor
Los Angeles, California 90012
(213) 972-8470
FAX (213) 972-8410

April 12, 2019

SUBJECT: LADOT DATA PROTECTION PRINCIPLES

The City of Los Angeles Department of Transportation (LADOT) works to deliver a safe, livable, and well-run transportation system throughout the region. Our vision is for all people in Los Angeles to have access to safe and affordable transportation choices that treat everyone with dignity and support vibrant, inclusive communities. As we work to achieve our responsibilities of safety, congestion relief, equity, and sustainability, we also have a responsibility to protect individual privacy and promote a transportation system free from discrimination and the exploitation of personal mobility data.

The Mobility Data Specification (MDS)¹ is designed to process vehicle data minimally necessary for our stated goals and to apply strong privacy protections and security protocols. For example, we categorize this data as Confidential under the City of Los Angeles Information Handling Guidelines -- which exempts the data from the California Public Records Act² -- and we apply strong access controls and de-identification measures to the data.

As part of its Dockless Mobility permitting process, the City of Los Angeles requires Mobility Service Providers (Operators) operating on the streets of Los Angeles to comply with the MDS. Such permitting rules set a consistent standard for the transfer, use, and protection of vehicle data from Operators to LADOT.

LADOT will apply the following data protection standards to all data obtained from Operators to carry out the City's and the Department's data protection responsibilities:

- 1) *Data categorization*: LADOT designates raw trip data as Confidential Information under the City of Los Angeles Information Technology Policy Committee (ITPC) Information Handling Guidelines. This long-standing policy for the City of Los Angeles governs the obligations of the City to protect all manners of data under its control. LADOT will withhold this Confidential Information as exempt from release under the California Public Records Act.

¹ <https://github.com/CityOfLosAngeles/mobility-data-specification>

²

https://static1.squarespace.com/static/57c864609f74567457be9b71/t/5bd2165471c10bf711f24edc/1540494932514/Information_Handling_Guidelines.pdf

- 2) *Data minimization*: LADOT will mandate data sets solely to meet the specific operational and safety needs of LADOT objectives in furtherance of its responsibilities and protection of the public right of way.
 - a. *Aggregation, obfuscation, de-identification, and destruction*: Where possible, LADOT will aggregate, de-identify, obfuscate, or destroy raw data where we do not need single vehicle data or where we no longer need it for the management of the public right-of-way.
 - b. Methodologies for aggregation, de-identification, and obfuscation of trip data will rely on industry best practices and will evolve over time as new methodologies emerge.

- 3) *Access limitation*: LADOT will limit access to raw trip data related to vehicles and vehicle trips to what is required for our operational and regulatory needs as established by the City Council.
 - 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, or other legal process. To be clear, the City will make no data available to law enforcement agencies through this process that is not already available to them from Operators now.
 - b. Similarly, the City will only allow access to raw trip data by contractors under the LADOT Third Party Master Data License Agreement which explicitly limits the use of raw trip data to purposes directed by LADOT and as needed for LADOT's operational and regulatory needs. LADOT will prohibit use of raw trip data for any non-LADOT purposes, including for data monetization or any third party purpose.
 - c. After completion of the Dockless Mobility Pilot, LADOT will create a publicly accessible transparency report discussing the types of third party requests for Dockless Mobility data that LADOT has received and how we have responded to those requests.

- 4) *Security*: The City will enact appropriate administrative, physical, and technical safeguards to properly secure and assure the integrity of data.
 - a. Los Angeles' formal information security program and the comprehensive set of security protections and standards established by the City will govern this data as it does all other city data, including but not limited to security incident and emergency response reporting.³
 - b. The City will conduct ongoing security testing to audit and improve security protections, consistent with the City of Los Angeles' information technology policies and practices.

- 5) *Transparency for the public*: The public deserve a clear description of the data used by LADOT and the ways such data is pertinent to the responsibility of protecting the public right-of-way. To that end, LADOT will publish a list of the data types collected via the MDS and the length of time that data is retained.

³ The current version is *City of Los Angeles Information Security Policy Manual* dated March 8, 2017.

- a. The City of Los Angeles 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.
- b. We share data via the City of Los Angeles [Open Data Portal](#). Before we publish any Dockless Mobility data to the Open Data Portal, LADOT will ensure the data is de-identified in accordance with established data protection methodologies.
- c. LADOT will not release any Dockless Mobility data on the Open Data Portal until data de-identification and destruction treatments are implemented.

Information Technology Policy Committee (ITPC)
Information Classification Policy



Information Classification Policy

Cyber Intrusion Command Center (CICC)

Policy Number: IT-016

Effective Date: 5/19/2016

MISSION

Mayor Eric Garcetti of the City of Los Angeles (hereafter referred to as the “City”) enacted Executive Directive No. 2 to protect the City’s digital assets, network infrastructure, and establish cybersecurity collaboration among the departments and law enforcement agencies. These digital assets must be kept secure and are entrusted to us by the citizens, businesses, and visitors of the City of Los Angeles. They may also contain personal information subject to State, Federal, and industry standards and mandates; the California Security Breach Notification Act protects all Personally Identifiable Information (PII); the Health Insurance Portability and Accountability Act (HIPAA) of 1996 that protects Personal Health Information (PHI); and Payment Card Industry Data Security Standards (PCI-DSS) that protects personal credit card information.

PURPOSE

Information is an asset of vital importance to the City. The City’s Information Classification Policy (Policy) takes reasonable and appropriate steps to identify and protect information originated or owned by the City, or entrusted to the City by others. All City information, regardless of format (written, electronic, verbal) is covered by this Policy, unless specifically exempted by the City Attorney in writing. Proper information classification, protection and handling are the responsibility of all City employees, including consultants, contractors and temporary employees working on behalf of the City.

Several documents comprise the execution of information classification for each department:

- The City’s Information Classification Policy — This Policy outlines the responsibilities of all City departments, agencies and employees under the City’s policy.
- The City’s Information-Handling Guidelines — This Information Handling Guidelines is a living document that defines certain information classes and handling guidelines.
- The City’s Open Data Policy – The Open Data Policy document establishes the City’s policy for making appropriate data freely available to companies, individuals, nonprofits, and other government agencies to promote government



transparency, accountability, public/private partnerships, technical innovation, and cross-department efficiencies.

- Privacy policy — The Privacy Policy outlines how information covered under various privacy laws should be handled.

INFORMATION CLASSIFICATION RESPONSIBILITIES

This section describes the roles and responsibilities assigned under the City's Information Classification Policy to all City employees, including consultants, contractors and temporary employees.

While every employee is responsible for proper information classification, protection and handling at a basic level, certain staff positions and City Departments require additional information classification responsibilities. These include the following.

Employee Responsibilities

- Understand the Information Handling Guidelines referenced by this Policy, and handle all information in accordance with this policy and guidelines.
- Immediately report an accidental or malicious breach of this Policy to the appropriate department or agency.

Management Responsibilities

- Communicate this Policy and ensure that employees receive appropriate training therefore.
- Ensure compliance with this Policy.
- Ensure appropriate notification of any breaches of this Policy, especially those breaches subject to privacy law or other regulated disclosure notifications.

Information Owner Responsibilities

- Ensure that the information they are responsible for is properly classified.
- Periodically review and assess information classifications, and adjust as required.

Legal Department Responsibilities

- Periodically review and assess information classifications, and adjust as required.
- Provide an "information nondisclosure agreement" template to information owners and others that can be used when information is provided to third parties.



Records Management Department Responsibilities

- Ensure that information storage, handling, retention and destruction guidelines outlined within this Policy are followed.

Ethics and Compliance Department Responsibilities

- Monitor compliance with this Policy.

REQUESTS FOR INFORMATION FROM THE PUBLIC, REGULATORY AUTHORITIES AND THE MEDIA

Public Requests - California Public Records Act (CPRA)

See Information Handling Guidelines

Regulatory Agency Requests

All requests for information received from any regulatory agency should be cleared through the City Attorney's Office.

Media Requests

All media requests for information should be directed to the respective. City Department's Public Relations, Communications, Media Relations or similar Department.

INFORMATION CLASSIFICATION ADMINISTRATION

Questions

All questions concerning this policy should be directed to City Attorney or the Mayor's Office

1. CICC CONTACT INFORMATION

Submit all inquiries and requests for future enhancements to the policy owner at:

Timothy Lee
Chief Information Security Officer
City of Los Angeles
200 N. Main Street, Room 1400
Los Angeles, CA 90012
Timothy.lee@lacity.org

2. REVIEW SCHEDULE AND REVISION HISTORY

This policy shall be reviewed and updated annually, as needed, or upon a major incident, whichever comes first.

Information Technology Policy Committee (ITPC)
Information Classification Policy



Version#	Effective Date	Edits Made
1.0		Policy first established

MASTER DATA LICENSE AND PROTECTION AGREEMENT

Between

CITY OF LOS ANGELES acting by and through the Los Angeles Department of Transportation

And

[INSERT COMPANY NAME]

This Master Data License and Protection Agreement (the “**Agreement**”) is made as of _____ (the “**Effective Date**”) by and between the City of Los Angeles acting by and through the Department of Transportation (“**LADOT**” or “**City**”), a municipal corporation of the State of California, and [INSERT COMPANY NAME] (“**Contractor**”), referred to herein collectively as “**Parties**” and individually as a “**Party**”.

WHEREAS, data relating to Mobility Service Providers (“**Provider**”) operating on the streets of Los Angeles will be made available to Contractor as a function of the City’s Mobility Data Specification (“**MDS**”) rules; and

WHEREAS, LADOT will enter into a contract with Contractor (the “**City Contract**”) pursuant to which Contractor will provide services to LADOT in order to store, process, analyze and present such data to facilitate, among other things, more informed transportation planning (“**Contracted Services**”).

NOW THEREFORE, in consideration of the covenants recited in this Agreement, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions

1.1 “City Data” means any and all data provided to the Contractor by or on behalf of the City, including as a result of Contractor’s performance of the Contracted Services, through the City’s MDS rules, set out at <https://github.com/CityOfLosAngeles/mobility-data-specification>, or any successor MDS, including, without limitation, any data received through any application programming interface (“**API**”); and any and all output, copies, reproductions, improvements, modifications, adaptations, derivations, aggregations, or translations thereof, even if such data was obtained by, transferred to, or reproduced, improved, modified, adapted, derived, or aggregated by Contractor prior to the effective date of this Agreement.

1.2 “Deliverables” means any reports, results, or analyses based on City Data required to be provided to the City as part of the Contracted Services under the City Contract.

1.3 [INSERT TOOLING PRODUCT TERM & DESCRIPTION]

2. License

2.1 City Data. The Parties agree that Contractor has no ownership of and, except as expressly provided in Section 2.5 of this Agreement, acquires no rights in City Data. As between the parties, City retains all right of ownership, title, and interest in and to City Data, including all intellectual property rights therein.

2.2 Except as specified in Section 2.2.1, City retains all right of ownership, title, and interest in and to any Deliverables and any work products originated and prepared using any part of City Data, including all intellectual property rights therein. Contractor hereby assigns to City all goodwill, copyright, trademark, patent, trade secret, and all other intellectual property rights worldwide in any work products originated and prepared using any part of City Data, except as specified in Section 2.2.1. Contractor further agrees to execute any documents necessary for City to perfect, memorialize, or record City’s ownership of rights provided herein.

2.2.1 Contractor, and its licensors, if any, retains all right, title, and interest in and to the [INSERT TERM FROM CLAUSE 1.3], and all intellectual property rights therein. In addition, Contractor, and its licensors, if any, retains all right, title, and interest in and to those work products that are mere improvements or modifications to the [INSERT TERM FROM CLAUSE 1.3], including updates to the functionality of tools provided therein.

2.3 Contractor agrees that a monetary remedy for breach of this Agreement may be inadequate, impracticable, or difficult to prove and that a breach may cause City irreparable harm. City may therefore enforce this requirement by seeking injunctive relief and specific performance, without any necessity of showing actual damage or irreparable harm. Seeking injunctive relief or specific performance does not preclude City from seeking or obtaining any other relief to which City may be entitled.

2.4 To the extent authorized in Section 9.6 of this Agreement, City acknowledges and agrees Contractor may use third-party subprocessors (“**Subprocessor**”) that may view, access, or possess City Data. Any subcontract entered into by Contractor related to the provision of Contracted Services with a Subprocessor shall include provisions sufficient to contractually bind Subprocessor such that City’s ownership, rights, and control of City Data and Contractor’s obligations to protect City Data, are preserved and protected as intended herein.

2.4.1 Contractor’s use of employees and independent contract staff to perform Contracted Services (“**Personnel**”) shall be formalized with such Personnel in writing and shall include employee policy or contract provisions sufficient to bind those Personnel such that Contractor’s obligations and City’s rights are preserved and protected as intended herein.

2.5 Subject to the confidentiality and other terms of this Agreement, LADOT grants Contractor a non-transferable (except as expressly contemplated by Section 9.5), non-exclusive, terminable at-will, license to use, analyze, host, store, and process City Data, for the purpose of performing the Contracted Services for LADOT. Contractor shall not use, analyze, host, store, or process City Data for any other purpose. Nothing in this Agreement shall prevent Contractor from improving the **[INSERT TERM FROM CLAUSE 1.3]** with City Data processed in the course of providing the Contracted Services, to the extent that no City Data is used, stored, or retained beyond the scope and term of this Agreement.

2.5.1 Contractor shall not exploit or commercialize City Data for any reason. Except as authorized in Section 4 of this Agreement, Contractor shall not disclose, sell, assign, or otherwise provide any part of City Data to any third party.

3. Data Protection.

3.1 In General. The protection of personal privacy and personally identifiable data shall be an integral part of the business activities of Contractor, and Contractor shall use all reasonable efforts to prevent inappropriate or unauthorized use of City Data at any time and safeguard the confidentiality, integrity, and availability of City Data and comply with the following conditions:

3.1.1. Contractor shall implement and maintain appropriate administrative, technical and organizational security measures in order to safeguard against unauthorized access, disclosure, or theft of City Data. Such security measures, as further described below, shall be reasonable and appropriate in light of the sensitivity and volume of City Data held by Contractor, the size and complexity of Contractor’s business, and the cost of available tools to improve security and reduce vulnerabilities. Contractor agrees to protect City Data using security means and technology necessary to meet this reasonableness standard and agrees, in any event, that such security measures shall be no less stringent than the measures Contractor applies to its own personal or confidential data.

3.1.2 Unless otherwise stipulated in writing, Contractor shall encrypt all City Data at rest and in transit with controlled access. The Contractor shall apply and support encryption solutions that are certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and keying material are not stored with any associated data. Whenever and wherever applicable, Contractor shall apply and support industry standards or better for tokenization, fraud-use protection, format-preserving encryption, and data encryption technology.

3.1.3 At no time shall any City Data be copied, disclosed, or retained by Contractor or any party related to Contractor, including its Subprocessors, for use in any process, publication, or transaction that is not specifically authorized by Section 4 of this Agreement or by the City in writing.

3.1.4 In accordance with Section 3.1.1, Contractor shall secure and protect all City Data from hacking, viruses, ransomware, and denial of service and related attacks. All City Data held by Contractor must be encrypted in accordance with Section 3.1.2. and Contractor shall take the measures required by this Section 3 to secure, and protect such City Data at all times.

3.2 Data, Development and Access-Point Location. Contractor shall provide its services to the City and its end users solely from data centers in the continental United States of America. Storage of City Data at rest shall be located in the continental United States of America. Contractor shall not allow its Personnel or Subprocessors to store City Data on portable devices, including personal computers, except for devices that are used and kept only at Contractor’s continental United States of America headquarters or data centers. Contractor may permit its Personnel and Subprocessors to access City Data remotely only as required to provide Contracted Services. Contractor shall neither access, nor allow a third-party access to City Data from any location outside of the continental United States

of America. Contractor shall not provide any services under this Agreement from a location outside of the continental United States of America, absent receipt of City's express approval.

3.2.1 Access Limitations. Contractor, insofar as this is possible, shall use precautions, including, but not limited to, physical software and network security measures, personnel screening, training and supervision, and appropriate agreements to:

3.2.1.1 Prevent anyone other than City, Personnel, and Subprocessors with a specific need to know, for a purpose authorized under this Agreement, from monitoring, using, gaining access to City Data;

3.2.1.2 Protect appropriate copies of City Data from loss, corruption, or unauthorized alteration; and

3.2.1.3 Prevent the disclosure of City and Contractor usernames, passwords, API keys, and other access control information to anyone other than authorized City personnel.

3.2.2 Security Best Practices. Contractor shall implement the following security best practices with respect to City Data and to any service provided:

3.2.2.1 Least Privilege: Contractor shall authorize access only to the minimum amount of resources required for a function.

3.2.2.2 Separation of Duties: The Contractor shall divide functions among its staff members to reduce the risk of one person committing fraud undetected.

3.2.2.3 Role-Based Security: The Contractor shall restrict access to authorized users and base access control on the role a user plays in the Contractor's organization.

3.2.3 Credential Restrictions. Contractor shall restrict the use of, and access to, administrative credentials for accounts and system services accessing City Data, to only those of Contractor's Personnel and Subprocessors whose access is essential for the purpose of providing the Contracted Services or performing obligations under this Agreement. Contractor shall require Personnel and Subprocessors to log on using an assigned user-name and password when administering City accounts or accessing City Data. These controls must enable Contractor to promptly revoke or change access in response to terminations or changes in job functions, as applicable. Contractor shall encrypt all passwords, passphrases, and PINs, using solutions that are certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and keying material are not stored with any associated data. Contractor will implement any City request to revoke or modify user access within twenty-four hours or the next business day of receipt of City's request. Contractor will disable user accounts after at most 10 consecutive invalid authentication attempts.

3.2.4 Physical and Environmental Security. Contractor facilities that process City Data must be housed in secure areas and protected by perimeter security such as barrier access controls including security guards and picture identification badges that provide a physically secure environment from unauthorized access, damage, and interference.

3.3 System Administration and Network Security.

3.3.1 Operational Controls. Contractor shall implement operational procedures and controls designed to ensure that technology and information systems are configured and maintained according to prescribed internal standards and consistent with applicable Industry Standard Safeguards. Examples of Industry Standard Safeguards are ISO/IEC 27002:2005, NIST 800-44, Microsoft Security Hardening Guidelines, OWASP Guide to Building Secure Web Applications, SOC 2 Type 2, and the various Center for Internet Security Standards. Moreover, Contractor shall use application security and software development controls designed to eliminate and minimize the introduction of security vulnerabilities.

3.3.2 Antivirus. Contractor shall have and maintain antivirus protection configured to automatically search for and download updates (daily, at a minimum) and perform continuous virus scans. Malware and threat detection must be updated continuously, and software patches provided by vendors must be downloaded and implemented in a timely manner. If Contractor is unable to implement these controls in a timely manner, Contractor shall notify City in writing.

3.3.3 Vulnerability Management and Patching. Contractor shall employ vulnerability management and regular application, operating system, and other infrastructure patching procedures and technologies designed to identify,

assess, mitigate, and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

3.3.4 Network Controls. Contractor shall have, shall implement, and shall maintain network security controls, including the use of firewalls, layered DMZs and updated intrusion, intrusion detection and prevention systems, reasonably designed to protect systems from intrusion or limit the scope or success of any attack or attempt at unauthorized access to City Data.

3.3.5 Logging and Monitoring. Unless prohibited by applicable law, Contractor shall, and shall require Subprocessors to, continuously monitor its networks and Personnel for malicious activity and other activity that may cause damage or vulnerability to City Data. Contractor shall maintain logs of administrator and operator activity and data recovery events related to City Data.

3.3.6 Changes in Service. Contractor shall notify the City of any changes, enhancement, and upgrades to the System Administration and Network Security, or changes in other related services, policies, and procedures, as applicable, which can adversely impact the security of City Data.

3.4 Policies, Assessments, and Audits.

3.4.1 Policies. Contractor shall, and shall require Subprocessors to, establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards, and procedures (collectively “Information Security Policy”), and communicate the Information Security Policy to all of its respective Personnel in a relevant, accessible, and understandable form. Contractor shall regularly review and evaluate the Information Security Policy to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks. Upon execution of this Agreement and thereafter within three (3) days of City’s request, Contractor shall make available for review by the City Contractor’s Information Security Policy and any related SOC audits or other evidence that Contractor has in place appropriate policies and procedures regarding information protection and security.

3.4.2 Vulnerability and Risk Assessments. At least annually, Contractor shall perform vulnerability tests and assessments of all systems that contain City Data. For any of Contractor’s applications that process City Data, such testing must also include penetration tests using intercept proxies to identify security vulnerabilities that cannot be discovered using automated tools, and code review or other manual verifications to occur at least annually.

3.4.3 Right of Audits by City/Security Review Rights. City and its agents, auditors (internal and external), regulators, and other representatives as City may designate, may inspect, examine, and review the facilities, books, systems, records, data, practices, and procedures of Contractor (and any Personnel and Subprocessors that Contractor may use) that are used in rendering services to City to verify the integrity of City Confidential Information and to monitor compliance with the confidentiality and security requirements for City Confidential Information. In lieu of an on-site audit, at City’s discretion and upon request by the City, the Contractor agrees to complete, within fourteen (14) days of receipt, an audit questionnaire provided by the City regarding the Contractor's data privacy and information security program. Contractor shall comply with all recommendations that result from such inspections, tests, and audits within reasonable timeframes.

3.5 Data Backup and Emergency Recovery. Contractor shall employ a multilayered approach to backups and disaster recovery including the use of a primary data center and a backup data center. Contractor shall perform both local and remote backups of the complete server infrastructure including server operating systems, applications, and data. Contractor shall perform Disaster Recovery Tests no less than semi-annually. Contractor shall maintain and comply with a reasonable written plan (the “DR Plan”) setting forth procedures for (a) mitigating disruption to systems during and after an earthquake, hurricane, other natural disaster, war, act of terrorism, act of cyberterrorism, and other natural or man-made disaster, including without limitation Force Majeure Events (as that term is used in PSC-6, Excusable Delays, of the Standard Provisions for City Contracts (Rev. 10/17)[v.3] (collectively, a “Disaster”); and (b) restoring Service functionality promptly after a Disaster. The DR Plan will include procedures no less protective than industry standard, and Contractor shall update the DR Plan as the industry standard changes.

3.6 Data Return and Destruction. At the conclusion of the Agreement and as instructed by City, Contractor shall (at its sole cost) return, delete, or destroy City Data then in its possession or under its control including, without limitation, originals, and copies of such City Data in accordance with Section 4.1.2. The following types of information are excluded from this requirement: (i) City Data that becomes a part of the public domain, including through court filings; and (ii) City Data that Contractor is required to maintain, by law, regulations, or by the terms

of this Agreement, but only for the time period required. For the avoidance of doubt, anything that is stored on routine backup media solely for the purpose of disaster recovery will be subject to destruction in due course rather than immediate return or destruction pursuant to this paragraph, provided that Personnel are precluded from accessing such information in the ordinary course of business prior to destruction.

3.6.1 Contractor shall implement and utilize appropriate methods to ensure the destruction of City Data. Such methods shall be in accordance with recognized industry best practices and shall leave no data recoverable on Contractor's computers or other media.

3.6.2 Certification of Destruction. Contractor agrees to certify that City Data has been returned, deleted, or destroyed from its systems, servers, off-site storage facilities, office locations, and any other location where Contractor maintains City Data within 45 days of receiving City's request that the information be returned, deleted, or destroyed. Contractor shall document its verification of data removal, including tracking of all media requiring cleaning, purging or destruction.

3.7 Data Breaches. Contractor shall notify City in writing as soon as reasonably feasible, but in any event within forty-eight hours, or if later, the next business day after Contractor's discovery of any unauthorized access of City Data or Contractor becoming reasonably certain that such unauthorized access has occurred (a "Data Breach"), or of any event that compromises the integrity, confidentiality or availability of City Data (a "Security Incident"), including, but not limited to, denial of service attack, and system outage, instability or degradation due to computer malware or virus. Contractor shall begin remediation immediately. Contractor shall provide daily updates if requested by City, and, in any event, reasonably frequent updates, regarding findings and actions performed by Contractor until the Data Breach or Security Incident has been resolved to City's satisfaction. Contractor shall conduct an investigation of the Data Breach or Security Incident and shall share a report of the investigation findings with City. At City's sole discretion, City and/or its authorized agents shall have the right to conduct an independent investigation of a Data Breach. Contractor shall cooperate fully with City and its agents in that investigation. If the City is subject to liability for any Data Breach or Security Incident that arises as a result of Contractor's negligent performance of services for the City or Contractor's breach of this Section 3, the Contractor shall fully indemnify and hold harmless the City and defend against any resulting actions.

3.8 This Section 3 applies only to City Data under Contractor's care; in Contractor's possession, custody, or control; or being accessed by Contractor.

3.9 City shall be responsible for the security of City usernames, passwords, API keys and other credentials required to access the [INSERT TERM FROM CLAUSE 1.3], to the extent such usernames, passwords, API keys and other credentials are in City's care, custody, or control. City shall be responsible for City's own disclosure of any City Data provided to City by Contractor or that City accessed through the [INSERT TERM FROM CLAUSE 1.3].

3.10 This Section 3 shall not apply to any data or information to which the confidentiality obligations set forth in Section 4.1.2 do not apply.

4. Confidentiality

4.1 City's Confidential Information. For purposes of this Section 4.1, "Confidential Information" means any nonpublic information whether disclosed orally or in written or digital media, received by Contractor that is either marked as "Confidential" or "Proprietary" or which the Contractor knows or should have known is confidential or proprietary information. City Data shall be treated as Confidential Information by Contractor under this Agreement, even if such data is not marked "Confidential" or "Proprietary" or was obtained by or transferred to Contractor prior to the effective date of this Agreement.

4.1.2 Protection of Confidential Information. Except as expressly authorized herein, Contractor shall (a) hold in confidence and not disclose any Confidential Information to third parties and (b) not use Confidential Information for any purpose other than fulfilling its obligations and exercising its rights under this Agreement or performing the Contracted Services. Contractor shall limit access to Confidential Information to Contractor Personnel and Subprocessors disclosed under Section 9.6, (1) who have a need to know such information for the purpose of Contractor performing its obligations or exercising its rights under this Agreement, or performing Contracted Services; (2) who have confidentiality obligations no less restrictive than those set forth herein; and (3) who have been informed of the confidential nature of such information. In addition, the Contractor shall protect Confidential Information from unauthorized use, access, or disclosure in the same manner that it protects its own proprietary

information of a similar nature, but in no event with less than reasonable care. At LADOT's request or upon termination or expiration of this Agreement, the Contractor will return to LADOT any Deliverables not provided to the City and Contractor will destroy (or permanently erase in the case of electronic files) all copies of Confidential Information, and Contractor will, upon request, certify to City its compliance with this sentence.

4.1.3 Exceptions. The confidentiality obligations set forth in Section 4.1.2 shall not apply to any Confidential Information that (a) is at the time of disclosure or becomes generally available to the public through no fault of the Contractor; (b) is lawfully provided to the Contractor by a third party free of any confidentiality duties or obligations; (c) was already known to the Contractor at the time of disclosure free of any confidentiality duties or obligations; or (d) the Contractor can demonstrate was independently developed by Personnel of the Contractor without reference to the Confidential Information. In addition, the Contractor may disclose Confidential Information to the extent that such disclosure is necessary for the Contractor to enforce its rights under this Agreement or is required by law or by the order of a court or similar judicial or administrative body, provided that (to the extent legally permissible) the Contractor promptly notifies LADOT in writing of such required disclosure, cooperates with LADOT if LADOT seeks an appropriate protective order, and the Contractor discloses no more information that is legally required.

4.2 Contractor's Confidential Information. For purposes of this Section 4.2, "Confidential Information" means any nonpublic information received by City that is either marked as "Confidential" or "Proprietary" at the time of disclosure, or, if provided orally, through verbal identification as confidential at the time of disclosure that, under the circumstances, a person exercising reasonable business judgment would understand to be confidential or proprietary. "Confidential Information" under this Section 4.2 is further limited to information that is a "trade secret," as defined in subdivision (d) of Section 3426.1 of the California Civil Code, or paragraph (9) of subdivision (a) of Section 499c of the California Penal Code, including but not limited to Contractor's (a) business plans, methods, and practices; (b) personnel, customers, and suppliers; (c) inventions, processes, methods, products, patent applications, and other proprietary rights; or (d) specifications, drawings, sketches, models, samples, tools, computer programs, technical information, or other related information, which is maintained by the Contractor as confidential.

4.2.2 Protection of Confidential Information. Except as expressly authorized herein, City shall hold in confidence and not disclose any Confidential Information to third parties and not use Confidential Information for any purpose other than fulfilling its obligations under this Agreement or the City Contract or realizing the benefits of the Contracted Services delivered thereunder. City shall limit access to Confidential Information to employees and contractors (1) who have a need to know such information for a purpose authorized under this Agreement; (2) who have confidentiality obligations no less restrictive than those set forth herein; and (3) who have been informed of the confidential nature of such information. In addition, City will protect Confidential Information from unauthorized use, access, or disclosure in the same manner that it protects its own proprietary information of a similar nature, but in no event with less than reasonable care. At Contractor's request, City will, to the extent permitted by the State of California's records retention laws, destroy (or permanently erase in the case of electronic files) all copies of Confidential Information, and City will, upon request, certify to Contractor its compliance with this sentence.

4.2.3 Exceptions. The confidentiality obligations set forth in Section 4.2.2 shall not apply to any Confidential Information that (a) is at the time of disclosure or becomes generally available to the public through no fault of the City; (b) is lawfully provided to the City by a third party free of any confidentiality duties or obligations; (c) was already known to the City at the time of disclosure free of any confidentiality duties or obligations; or (d) the City can demonstrate was independently developed by personnel of the City without reference to the Confidential Information. In addition, the City may disclose Confidential Information to the extent that such disclosure is necessary for the City to enforce its rights against Contractor under this Agreement or as required by law, including the California Public Records Act (CPRA), or by the order of a court or similar judicial or administrative body, provided that (to the extent legally permissible) the City promptly notifies Contractor in writing of such required disclosure and the City discloses no more information than is legally required.

4.2.4 Contractor undertakes and agrees to defend, indemnify and hold harmless City and any of City's boards, officers, agents, and employees from and against all suits, claims, and causes of action brought against City for City's refusal to disclose Confidential Information to any person making a request pursuant to the CPRA. Contractor's obligations herein include, but are not limited to, all reasonable attorney's fees (both in house and outside counsel), reasonable costs of litigation incurred by City or its attorneys (including all reasonable actual, costs incurred by City, not merely those costs recoverable by a prevailing party, and specifically including

reasonable costs of experts and consultants) as well as all damages or liability of any nature whatsoever arising out of any such suits, claims, and causes of action brought against City, through and including any appellate proceedings. Contractor's obligations to City under this indemnification provision shall be due and payable on a monthly, on-going basis within thirty (30) days after each submission to Contractor of City invoices for all fees and costs incurred by City, as well as all damages or liability of any nature. Contractor shall receive prompt written notice from City within five (5) business days of receipt of any (1) communication to City challenging City's refusal to disclose Confidential Information, and (2) any complaint or petition to the court challenging City's refusal to disclose Confidential Information. Further should Contractor choose to intervene in any court action relating to the City's refusal to disclose Contractor's information, City shall not oppose Contractor's motion to intervene. Contractor shall have no obligations to City under this provision in any circumstance where Contractor provides written confirmation to City that 1) all of the requested records at issue are not Confidential Information and 2) City may release said records to the requester.

4.3 Compliance with Privacy Laws. Contractor is responsible for ensuring that Contractor's performance of its obligations and exercise of its rights under this Agreement complies with all applicable local, state, and federal privacy laws and regulations, as amended from time to time. If this Agreement or any practices which could be, or are, employed in performance of this Agreement become inconsistent with or fail to satisfy the requirements of any of these privacy laws and regulations, City and Contractor shall in good faith execute an amendment to this Agreement sufficient to comply with these laws and regulations and Contractor shall complete and deliver any documents necessary to show such compliance. The City acknowledges and agrees that Contractor is not responsible for giving any notices to or obtaining any consents from any other party in order for Contractor to process the City Data as contemplated by this Agreement.

5. Warranties. Contractor represents and warrants that:

5.1 Disabling Code. No software or services to which the City is provided access and use hereunder contains any undisclosed disabling code (defined as computer code designed to interfere with the normal operation of the software or the City's hardware or software) or any program routine, device or other undisclosed feature, including but not limited to, a time bomb, virus, drip-dead device, malicious logic, worm, Trojan horse, or trap door which is designed to delete, disable, deactivate, interfere with or otherwise harm the software or the City's hardware or software.

5.2 Virus/Malicious Software. Contractor has used its best efforts to scan for viruses within Contractor's networks and information systems, and no malicious system will be supplied under this Agreement.

5.3 Information Security. Contractor's information security procedures, processes, and systems will at all times meet or exceed (i) the requirements of this Agreement; and (ii) all applicable information security and privacy laws, and legally binding standards, rules, and requirements related to the collection, storage, processing, and transmission of personally identifiable information.

6. Indemnification; Limitation of Liability

6.1 Indemnification. Except for the active negligence or willful misconduct of City, or any of its boards, officers, agents, employees, assigns, and successors in interest, Contractor shall defend, indemnify, and hold harmless City and any of its boards, officers, agents, employees, assigns, and successors in interest from and against all lawsuits and causes of action, claims, losses, demands, and expenses, including, but not limited to, attorney's fees (both in house and outside counsel), reasonable cost of litigation (including all actual litigation costs incurred by City, including but not limited to, costs of experts and consultants), damages, or liability of any nature whatsoever, for death or injury to any person, including Contractor's Personnel and agents, or damage or destruction of any property of either party hereto or of third parties, arising in any manner by reason of an act, error, or omission by Contractor, Subprocessors, subcontractors, or their boards, officers, agents, Personnel, assigns, and successors in interest. The rights and remedies of City provided in this Section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Agreement. This provision will survive expiration or termination of this Agreement.

6.2 Limitation of Liability. Neither party shall be liable hereunder for special, indirect, consequential, or incidental losses or damages including, but not limited to, lost profits, lost or damaged data, failure to achieve cost savings, or the failure or increased expense of operations, regardless of whether any such losses or damages are characterized as arising from strict liability or otherwise, even if a party is advised of the possibility of such losses or

damages, or if such losses or damages are foreseeable. The limitations of Contractor's liability in this Section 6.2 do not apply to: (a) Contractor's breach of Section 4 (Confidentiality), and (b) Contractor's obligations in Section 6.1 (Indemnity).

6.3 Liability Cap. In no event shall either party's liability arising out of or relating to this Agreement exceed three times (3x) the fees paid under the City Contract during the twelve (12) months preceding the act, omission, or occurrence giving rise to such liability. The cap on liability in this Section 6.3 does not apply to Contractor's obligations under Section 3 (Data Protection), Section 4 (Confidentiality), and Section 6 (Indemnification),

7. Data Disclaimer. All data provided by or on behalf of City pursuant to this Agreement are provided "as is." City makes no representation or warranty, express or implied, regarding the data's accuracy, completeness or use. There are no express or implied warranties of merchantability or fitness for a particular purpose, or that the use of the data will not infringe any patent, copyright, trademark, or other proprietary rights. Without limiting the generality of the foregoing, City does not represent or warrant that the data or access to it will be uninterrupted or error free.

8. Term

8.1 Term. The term of this Agreement shall be coextensive with the City Contract.

8.2 Survival. The provisions of Sections 2, 3, 4, and 6 will survive the termination or expiration of this Agreement.

8.3 Retroactive Application. The Parties agree that, to the extent permitted by applicable law, the provisions of Sections 2, 4, 6, and 7 of this Agreement shall be applied retroactively to any and all Contracted Services performed by Contractor, and any of its Personnel or Subprocessors, even if those acts and actions occurred or were in progress prior to the effective date of this Agreement.

9. General Provisions

9.1 Governing Law and Venue. This Agreement and any action related thereto will be governed and interpreted by and under the laws of the State of California, without giving effect to any conflicts of laws principles that require the application of the law of a different jurisdiction. Each party hereby expressly consents to the exclusive personal jurisdiction and venue in the state and federal courts of Los Angeles County, California for any lawsuit filed there against it by the other party arising from or related to this Agreement.

9.2 Export. Contractor agrees not to export, report, or transfer, directly or indirectly, any City Data, or any products utilizing such data, in violation of United States export laws or regulations. Without limiting the foregoing, Contractor agrees that (a) it is not, and is not acting on behalf of, any person who is a citizen, national, or resident of, or who is controlled by the government of any country to which the United States or other applicable government body has prohibited export transactions (e.g., Iran, North Korea, etc.); (b) is not, and is not acting on behalf of, any person or entity listed on a relevant list of persons to whom export is prohibited (e.g., the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons, the U.S. Commerce Department Denied Persons List or Entity List, etc.); and (c) it will not use any City Data for, and will not permit any City Data to be used for, any purpose prohibited by applicable law.

9.3 Severability. If any provision of this Agreement is, for any reason, held to be invalid or unenforceable, the other provisions of this Agreement will remain enforceable and the invalid or unenforceable provision will be deemed modified so that it is valid and enforceable to the maximum extent permitted by law.

9.4 Waiver. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

9.5 No Assignment. Except as provided in Section 9.6, Contractor will not assign, subcontract, delegate, or otherwise transfer this Agreement, or its rights and obligations herein, without obtaining the prior written consent of LADOT, and any attempted such assignment, subcontract, delegation, or transfer in violation of the foregoing will be null and void.

9.6 Subprocessors. City acknowledges and expressly agrees that Contractor may retain Subprocessors in the course of providing Contracted Services. Contractor shall make available to City a current list of Subprocessors and

their respective services immediately upon execution of this Agreement. When Contractor engages any new Subprocessor after the execution of this Agreement, Contractor will notify LADOT of such Subprocessor at least 30 days before the Subprocessor accesses or processes any City Data. Any and all Subprocessors shall be bound by the obligations of Contractor under this Agreement; notwithstanding the foregoing, Contractor remains responsible for compliance of any such Subprocessor with the terms of this Agreement.

9.7 Notices. All notices required to be given pursuant to the terms of this Agreement shall either be personally delivered or delivered by certified mail return receipt requested to:

If to LADOT:

Seleta J. Reynolds, General Manager
Los Angeles Department of Transportation
100 South Main Street, 10th Floor
Los Angeles, California, 90012

With copies to:

Marcel Porras, Chief Sustainability Officer
Los Angeles Department of Transportation
100 South Main Street, 10th Floor
Los Angeles, California, 90012

If to Contractor:

[INSERT NOTICE ADDRESS]

Attention: [INSERT NAME/TITLE/EMAIL]

Or to any such other address as the parties may designate in writing, from time to time. All mailed notices shall be deemed received three days after being deposited in the U.S. mail.

9.8 Counterparts. This Agreement may be executed in one or more counterparts, each of which will be deemed an original and all of which will be taken together and deemed to be one instrument.

9.9 Entire Agreement. No-shrink-wrap, click-wrap, privacy policy, or other terms and conditions or agreements (“Additional Contractor Software Terms”) provided with any products, services, documentation, or software hereunder, or under the Contracted Services agreements, shall be binding on the City, even if use of the foregoing requires an affirmative “acceptance” of those Additional Contractor Software Terms before access is permitted. All such Additional Contractor Software Terms will be of no force or effect and will be deemed rejected by the City in their entirety. This Agreement is the final, complete and exclusive agreement of the parties with respect to the licensing, use and protection of City Data, and supersedes and merges all prior discussions between the Parties with respect to such subject matters. No modification of or amendment to this Agreement, or any waiver of any rights under this Agreement, will be effective unless in writing and signed by an authorized signatory of each Party.

In Witness Whereof, the parties have caused their duly authorized representatives to execute this Agreement as of the Effective Date.

THE CITY OF LOS ANGELES

[INSERT COMPANY NAME]

By: _____

Seleta J. Reynolds

General Manager

Department of Transportation

Date: _____

By: _____

Date: _____

APPROVED AS TO FORM:

MICHAEL N. FEUER, City Attorney

By**: _____

By: _____

Title: _____

Date: _____

Date: _____

CITY OF LOS ANGELES

CALIFORNIA

Seleta J. Reynolds
GENERAL MANAGER



ERIC GARCETTI
MAYOR

DEPARTMENT OF TRANSPORTATION

100 South Main Street, 10th Floor
Los Angeles, California 90012
(213) 972-8470
FAX (213) 972-8410

DOCKLESS ON-DEMAND PERSONAL MOBILITY RULES & GUIDELINES VERSION 0.2

Goal

In the last decade, coinciding with the introduction of the smartphone, the City of Los Angeles (“City”) has seen an explosion in new mobility products and services. Acceleration of shared mobility, artificial intelligence and machine learning, electrification and solar power, GPS and big data combined to change the mobility landscape more than in the previous 40 years. The City is taking a proactive approach to integrate these technologies into the fabric of its transportation system. This document, and the beta program described herein, is part of a broader effort to understand dockless, on-demand technology and the implications for the City and its citizens. This effort empowers the City with the tools to make informed, data-driven decisions to ensure transportation options are safe for City residents, and to deliver on the City’s goals of socioeconomic and racial equity.

Definitions

City means the City of Los Angeles.

Customer means a person or organization that buys a mobility service from an Operator.

Municipality means a city or a town that has corporate status and local government.

Program means the Dockless On-Demand Personal Mobility Beta within the City.

Operator means a company that operates a Mobility-as-a-Service company within a Municipality.

Vehicle means an Operator device that is used or intended to be used by a person to move from one physical point to another.

Purpose

The purpose of the Dockless On-Demand Personal Mobility Rules & Guidelines is to establish requirements to govern and permit the operation of a Program in the City.

Duration

- a) The Program is intended to last 6 months from issuance of the first Program permit. The City reserves the right to modify the Program in duration or scope based on the information it collects from the Program.

- b) Notwithstanding the duration of the Program, Operator Program permits must be renewed yearly. Permit requirements may be adjusted yearly to accommodate changing technology, needs, and priorities.

Modifications

At its discretion, the City reserves the right to amend, modify or change the terms and conditions within the Program.

Relationship to City

- a) In rendering service hereunder, the Operator shall be and remain an Independent Contractor. It is expressly understood and acknowledged by the parties that any amounts payable hereunder shall be paid in gross amount, without reduction for penalties, taxes, or charges. Operators are responsible for assuming any applicable federal or state withholding taxes, estimated tax payments, or any other fees or expenses whatsoever.
- b) Permits issued under this Program are not to be assigned or delegated to a substitute provider, a successor in interest, or a purchaser of the permit without express written permission by the City.
- c) The City reserves the right to terminate permits at any time and require the Operator to remove their entire fleet of Vehicles from City streets. An Operator will have 30 days to remove the entire fleet from City streets.

Non-transferability

- a) This permit may not be transferred to another party or entity without the express written permission of the City of Los Angeles.

Indemnification

AGREEMENT TO INDEMNIFY, DEFEND AND HOLD HARMLESS ("Agreement")

By obtaining this permit, Operator agrees to defend, indemnify, and hold harmless the City, its officers, elected or appointed officials, employees, agents, and volunteers from and against any and all claims, damages, losses, expenses, fines, penalties, judgments, demands, and defense costs (including, without limitation, actual, direct, out-of-pocket costs and expenses, and amounts paid in compromise, settlement, or judgment, and reasonable legal fees arising from any claim or litigation of every kind or nature or liability of any kind or nature including civil, criminal, administrative or investigative) arising out of, in connection with, or which are in any way related to, the City's issuance of or decision to approve the Operator's Permit, the process used by the City in making decisions, Operator's participation in the Shared Mobility Device Pilot Program, the Operator's (including its officers, managers, employees, contractors, agents, and volunteers) business conduct and operations, any violation of any laws by the Operator (including its officers, managers, employees, contractors, agents, and volunteers) or its users, or any bodily injury including death or damage to property arising out of or in connection with any use, misuse, placement or misplacement, including but not limited to placement or misplacement resulting in alleged violations of the Americans with Disabilities Act (ADA), of

Operator's device, property or equipment by any person, except such loss or damage which was caused by the sole willful misconduct of the City. Operator will conduct all defenses pursuant to this Agreement at Operator's sole cost and expense, and City shall reasonably approve selection of the counsel to represent City as proposed by Operator. This Agreement shall apply to all claims and liability regardless of whether any insurance of Operator, its affiliates or other parties are applicable thereto. The policy limits of any insurance of Operator, its affiliates or other parties are not a limitation upon the obligation of Operator, including without limitation, the amount of indemnification to be provided by Operator. The provisions of this section shall survive the termination of this Agreement.

SEVERABILITY AND GOVERNING LAW. If any provision or portion of this Permit shall be held by a court of competent jurisdiction to be invalid, void, or otherwise unenforceable, the remaining provisions shall remain enforceable to the fullest extent permitted by law. This Permit shall be governed by and construed and enforced in accordance with the laws of the State of California applicable to contracts made and to be performed in California.

AMENDMENT/INTERPRETATION OF THIS PERMIT. This Permit represents the entire understanding of the parties as to those matters contained herein. No prior oral or written understanding shall be of any force or effect with respect to those matters covered hereunder. The City, at its sole discretion pursuant to Los Angeles Municipal Code Section 71.29, may amend any term or condition of this Permit as necessary during the Pilot Program. This Permit shall not be interpreted for or against any party by reason of the fact that such party may have drafted this Permit or any of its provisions.

CPRA INDEMNITY LANGUAGE. ("Company") undertakes and agrees to defend, indemnify and hold harmless the City of Los Angeles and any of its boards, officers, agents, and employees (collectively, the "City") from and against all suits, claims, and causes of action brought against the City for the City's refusal to disclose Company's trade secrets or other technical or financial information, or Company's personally identifiable customer data, to any person making a request pursuant to the State of California Public Records Act (California Government Code Section 6250 et seq.). Company's obligations herein include, but are not limited to, all reasonable attorney's fees (both in house and outside counsel), reasonable costs of litigation incurred by the City or its attorneys (including all actual, costs incurred by the City, not merely those costs recoverable by a prevailing party, and specifically including costs of experts and consultants) as well as all damages or liability of any nature whatsoever arising out of any such suits, claims, and causes of action brought against the City, through and including any appellate proceedings. Company's obligations to the City under this indemnification provision shall be due and payable on a monthly, on-going basis within thirty (30) days after each submission to Company of the City's invoices for all fees and costs incurred by the City, as well as all damages or liability of any nature. Company shall receive prompt notice from the City of any (1) communication to the City challenging the City's refusal to disclose Company's information, and (2) any complaint or petition to the court challenging the City's refusal to disclose Company's information. Further should Company choose to intervene in any court action relating to the City's refusal to disclose Company's information, the City shall not oppose Company's motion to intervene. Company shall be discharged of its obligations to the City under this provision in any circumstance where Company provides written confirmation to the City that 1) all of the requested records at issue are not Company trade secrets, technical, financial or other similar information or personally identifiable customer data and 2) the City may release said records to the requester.

Insurance Requirements

- a) All permitted Operators shall have commercial general liability insurance, including contractual liability, and property damage insurance written by an insurance company authorized to do business in the State of California, or approved by the California Department of Insurance as a surplus lines insurer eligible to do business in California, rated VII, A- or better in Best's Insurance Guide (or an alternate guide acceptable to City and Department if a Best's Rating is not available) with Licensee's normal limits of liability, but not less than Five Million Dollars (\$5,000,000) for injury or death to one or more persons out of each accident or occurrence and Five Million Dollars (\$5,000,000) for bodily injury and property damage for each occurrence. Each policy shall name the "City of Los Angeles, its officers, agents and employees" as Primary additional insureds.
- b) Workers' Compensation insurance as required by the State of California, with Statutory Limits and Employers' Liability Insurance with limits of no less than \$1,000,000 per accident for bodily injury or disease.
- c) Operator shall maintain an umbrella insurance policy providing coverage in excess of its primary general liability, employer's liability and automobile liability policies in an amount not less than \$5,000,000 per occurrence. The city of Los Angeles must be named as additional insured.
- d) Automobile insurance with limits of liability not less than One Million Dollars (\$1,000,000) covering injuries or death resulting from each accident or claim arising out of any one claim or accident. This insurance shall cover all owned, non-owned, and/or hired automobiles. Each policy shall name the "City of Los Angeles, its officers, agents and employees" as Primary additional insureds.
- e) All Operators shall have a performance bond of \$80/Vehicle. The form of the bond shall be approved by the City. These funds shall be accessible to the City for costs that may be incurred for, including but limited to, removing and storing improperly parked Vehicles and if an Operator fails to remove the Vehicles when its permit is terminated. If an Operator increases the size of their fleet, the performance bond shall be adjusted appropriately before deploying additional Vehicles.

Operator Responsibilities

- a) Operators seeking to participate in the Program will register with the Office of Finance within the City for business tax compliance. Operators can either register on-line or in person at one of the public service centers.
- b) Operators must be in compliance and in good standing with tax payments or the permit may be revoked or not eligible for renewal the following year.

Universal Requirements

- a) No Vehicle shall be put in service until the appropriate Program permit is obtained from the City.
- b) Program permits shall be valid for a maximum of six (6) months from the date of issue and all issued Program permits will expire on the same date.

- c) Operators are advised that application for a Program permit does not guarantee issuance of a Program permit.

Data Protection and Privacy

- a) As directed by the Los Angeles City Council (CF 19-1355)- the City will apply LADOT's data protection principles to all data obtained from Operators to carry out the City's and the Department's data protection responsibilities including, but not limited to, data categorization, data minimization, access limitation, security, and transparency to the public.

Vehicle Identification

- a) Every Vehicle shall have a unique identifier that is readily visible to the Customer or any member of the public. Operators shall provide easily visible contact information, including toll-free phone number and e-mail address, on each Vehicle for the Customers or members of the public to make relocation requests or to report other issues with the vehicles.

Safety

- a) All bicycles shall meet the safety standards outlined in ISO 43.150 – Cycles, as well as the standards outlined in Code of Federal Regulations Title 16, Chapter II, Subchapter C, Part 1512 – Requirements for Bicycles. In addition, all bicycles shall meet the standards established in CVC section 21201, including for lighting during operation in darkness.
- b) Electric-assist bicycles shall be “Class 1” or “Class 2” electric bicycles only, as defined in California Vehicle Code (CVC) Section 312.5 Additionally, the City reserves the right to terminate any permit issued under this Program if the battery or motor on an electric-assist bicycle is determined by the City to be unsafe for public use.
- c) An electric scooter shall be any two-wheeled device that has handlebars, has a floorboard that is designed to be stood upon when riding, and is powered by an electric motor or other power source. This device may also have a driver seat that does not interfere with the ability of the rider to stand and ride and may also be designed to be powered by human propulsion. A motorcycle, as defined in Section 400 of the California Vehicle Code, a motor-driven cycle, as defined in Section 405 of the California Vehicle Code, or a motorized bicycle or moped, as defined in Section 406 of the California Vehicle Code, is not an electric scooter.
- d) Electric scooters shall be incapable of reaching a top speed of greater than 15 mph. LADOT reserves the right to revise the speed limit based on collision and injury data.
- e) Electric-assist bicycle systems shall have visible language that notifies the user that:
- Helmet use is encouraged while riding a bicycle;
 - Riders shall yield to pedestrians; and
 - When riding on-street, follow the rules of the road, following all motor-vehicle laws and ordinances in the City of Los Angeles.
- f) Electric scooter systems shall have visible language that notifies the user that:
- Helmets use is encouraged when operating an electric scooter;
 - Riders shall yield to pedestrians;

- When riding on-street, follow the rules of the road, following all motor-vehicle laws and ordinances in the City of Los Angeles;
 - “No Riding On Sidewalks” (minimum 48-point font) located on the platform of every scooter; and
 - Customer must be a minimum of 18 years old with Driver’s License to operate Vehicle.
- g) Electric scooter systems shall have always-on front and back lights that are visible from a distance of at least 300 feet under normal atmospheric conditions at night. Front and rear lights must stay illuminated for at least 90 seconds after the vehicle has stopped during a trip.

Fleet Size

- a) All Operator applicants to the Program shall include the total fleet size in their application.
- b) All Operators shall have a minimum fleet of 500 Vehicles; Operators shall meet this fleet size within four weeks of the date of issuance of their Program permit.
- c) All Operators using only adaptive bicycles for persons with disabilities (non-electric) shall have no minimum fleet size. If using any combination of dockless bicycles (non-electric), electric-assist bicycles, or electric scooters with adaptive bicycles, Operator will be required to meet the 500-vehicle minimum.
- d) Operators must reserve a minimum of 50 percent of their fleet size for electric vehicles unless providing adaptive bicycles (non-electric) for persons with disabilities. Operators that do not provide 50 percent of their fleet size for electric vehicles must reserve a minimum of 1 percent of their fleet size for adaptive bicycles.
- e) Operators shall notify the City and submit a revised Permit Application to request an increase in total permitted fleet size prior to deploying new Vehicles into service.
- f) The overall fleet size per Operator may not exceed 3,000 Vehicles, with the exception if the Operator is adding vehicles within disadvantaged communities as defined by the CalEnviro Screen 3.0
- g) Operators may add up to 2,500 vehicles in communities that scored at or above the 75th percentile as defined by the CalEnviroScreen 3.0. Operators may be allowed up to 5,000 additional vehicles in disadvantaged communities in the San Fernando Valley.
- h) Additional vehicles after the total 10,500 fleet maximum may be permitted at the discretion of the General Manager and may depend on factors related to performance and Program compliance. General Manager to publish the criteria used to evaluate expansion permits.
- i) The General Manager may reduce the permitted number of vehicles in the case of demonstrated Program noncompliance and/or nonperformance by permittee

Compliance with Mobility Data Specification

- a) All Operators shall abide by the Mobility Data Specification (“Specification”) as published online at <https://github.com/openmobilityfoundation/mobility-data-specification> and updated from time to time.
- b) As part of the Program permit application process (initial or renewal), all Operators shall demonstrate support for v1.1 or any subsequent version of the LADOT MDS API Technical Compliance Overview.
- c) The City may conduct maintenance on, stop providing, and/or change the method of access to the Services, Software, and/or Content outlined in the LADOT MDS Compliance Guidelines at any time, with or without notice to the Operator. For avoidance of doubt, the City, in its sole discretion, may temporarily or permanently suspend Operator’s access to the Services, Software, and/or Content under this Agreement.

Service Area and Geo-Fencing

- a) The Program is valid only for operations within the City’s rights-of-way.
- b) At the City’s discretion, additional operating zones may be established including locations within parks, publicly-accessible plazas, on-street parking spaces, off-street parking lots/garages, or campuses. However, permission to do so shall require coordination with the appropriate department, agency, or property owner; and shall be communicated to the Customer through signage approved by the respective entity and/or through the Operator’s mobile and web application.
- c) The City reserves the right to determine where Vehicle parking is prohibited or to create geo-fenced stations within certain areas where Vehicles shall be parked. The City will make this information available via MDS policy end-point or alternative method.
- d) The City shall maintain geographic parking boundaries for Operators and make these available via the MDS policy end-point or alternative method.

Special Operations Zones (SOZ)

- a) At the City’s discretion, Special Operations Zones may be established to address neighborhood-specific concerns including, but not limited to, oversaturation, operating regulations, equity, fleet caps, and parking behavior. These Special Operations Zones will be published via the MDS policy end-point.

Marketing / Advertising

- a) Operator shall not display third party advertising on their Vehicles.

Operator Customer Service

- a) All Operators shall provide a mechanism for Customers to notify the Operator that there is a safety or maintenance issue with the Vehicle.
- b) Operator shall maintain an updated organizational chart with contact information of their operations team and advise the LADOT Program Manager of any changes within 48 hours.

Reporting / Data Sharing

- a) Raw data supplied by an Operator shall be held confidentially between the City and the Operator to the extent that is permitted by law. However, summaries, program utilization data, and trend data may be made public.
- b) Personally Identifiable Information on Customers collected by Operators may not be transmitted to, processed or stored at a destination outside of the United States.
- c) The City is permitted to use all data the Operator provides in accordance with the Program including, but not limited to, displaying real-time data and real-time Vehicle availability data to the public. Third parties are permitted to republish any data the City publishes.
- d) During the Program, Operators shall distribute to their Customers a City-provided customer survey at a maximum frequency of quarterly.

Operations & Maintenance

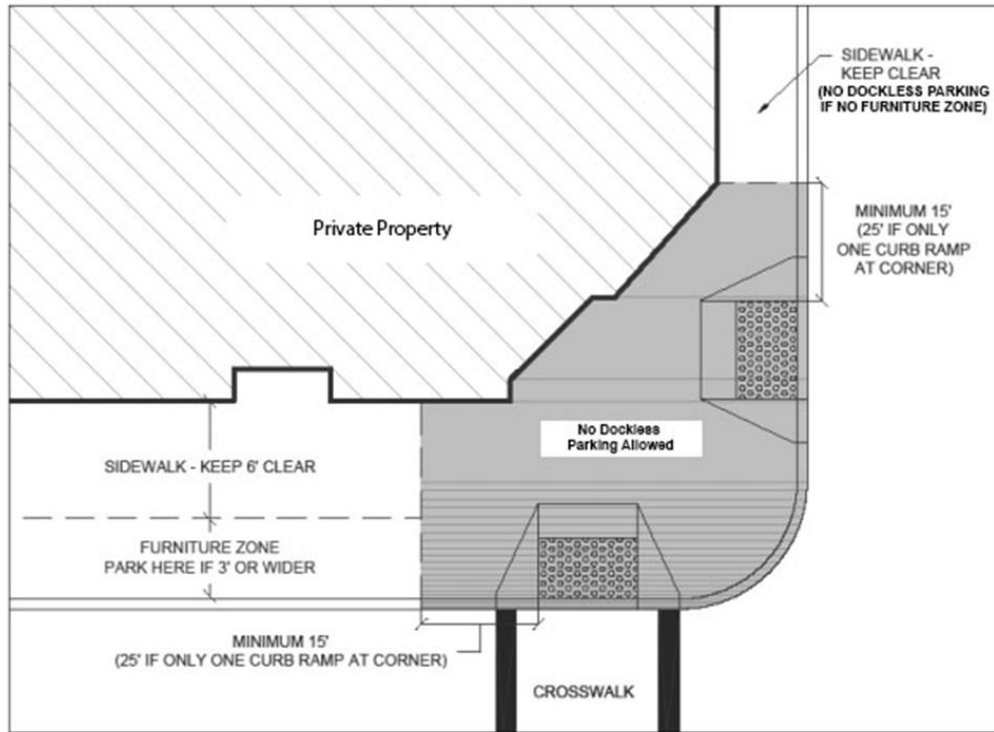
- a) All Operators shall have a staffed operations center in the City and a 24-hour contact person available for emergency removals .
- b) Operator shall remedy devices parked incorrectly or are inoperable within two hours of being notified by the City from 7am to 10pm daily.
- c) Operator shall remedy devices parked incorrectly or are inoperable within two hours of being notified by the general public from 7am to 10pm daily.
- d) An Operator shall repair any inoperable Vehicle or any Vehicle that is not safe to operate before returning the Vehicle into revenue service.
- e) If LADOT or any other City department or office incurs any costs addressing or abating any violations of this agreement, or incurs any costs of repair or maintenance of public property, and potentially upon receiving written notice of City costs, the Operator shall reimburse the City for such costs within thirty days of receipt of an invoice detailing such costs.
- f) Operators will attend an on-site meeting with City staff to discuss the program and show a demonstration Vehicle that will be deployed prior to permit approval.
- g) Operators shall submit maintenance schedule and maintenance logs to the City via the report-maintenance API or MDS v0.1 endpoint.

Parking

- a) For any permitted location response obtained from the MDS policy end-point, an Operator shall ensure their Vehicles are parked in the landscape/furniture zone of the sidewalk, preferably to a bicycle rack or in another area specifically designated for bicycle parking. Operators shall inform Customers on how to properly park a Vehicle.
- b) Every Vehicle may be equipped with a locking mechanism to lock to a fixed object preferably a bicycle rack, or shall have smart technology equipment to prevent theft, technology identifying vehicle is upright and properly parked, and GPS tracking. However, LADOT shall reserve the right to require operators to include a locking mechanism to lock to a fixed object at any time. Operators shall remove electric scooters from the public right-of-way on a daily basis.

- c) All dockless vehicles within a reasonable timeframe but no longer than 3 months after issuance of the latest Program permit shall come equipped with technology that would prevent operators from ending a ride if the vehicle is not standing upright.
- d) Operators shall ensure their Vehicles are not parked in a way that impedes the regular flow of travel in the public way, or in a way that impedes the clearance on sidewalks needed for ADA compliance. Legal parking includes the landscape/furniture zone and any bicycle rack in the public right of way.
- e) Operators are responsible for informing Customers how to park the Vehicle correctly. Operators will provide a “Parking Plan” on how they will incentivize Customers to park safely and correctly and will be responsible for passing on fees and disincentives for Vehicles parked illegally outside of the “furniture zone” and outside of “geo-fenced area”.
- f) Restrictions to eligible parking zones on sidewalks shall be as follows:
- Vehicles shall not be parked at the corners of sidewalks nor at any crosswalk, curb ramp, or within any feature that serves as an accessible element such as landings, areas of refuge, detectable warning surfaces, or any other physical feature that may be required for mobility.
 - Vehicles shall not be parked on blocks where the landscape/furniture zone is less than 3 feet wide, or where there is no landscape/furniture zone.
 - On blocks without sidewalks, Vehicles may be parked if the travel lane(s) and 6-foot pedestrian clear zone are not impeded.
 - The City reserves the right to determine certain block faces where dockless parking is prohibited.
 - Vehicles can only be parked on hard surfaces within the landscape/furniture zone (e.g. concrete, asphalt).
 - Any Vehicle that is parked in one location for more than 5 consecutive days without moving may be removed by the City’s Bureau of Sanitation and taken to a City facility for storage at the expense of the Operator. Bureau of Sanitation shall invoice the violating Operator for fees incurred.
 - Vehicles shall not be parked in the landscape/furniture zone adjacent to or within:
 - Parklets;
 - Transit zones, including bus stops, shelters, passenger waiting areas and bus layover and staging zones, except at existing bicycle racks;
 - Loading zones;
 - Disabled parking zone, or any other accessible route that would otherwise create a barrier to accessibility;
 - Locked to street furniture that requires pedestrian access (for example - benches, parking pay stations, bus shelters, transit information signs, etc.);
 - Curb ramps;
 - Red curb zones;
 - Entryways; and
 - Driveways.
- g) Vehicles shall be upright when parked.

- h) Operators shall work with each individual Council District if additional parking is required, which includes bicycle racks and/or bicycle corrals.
- i) Vehicles shall not be parked within 15' of street corner pedestrian ramps (25' if there is only a single pedestrian ramp). Refer to graphic below:



Enforcement & Termination Grounds

- a) If data is falsified or the City suspects dishonest reporting, the City reserves the right to revoke the Program permit. In the case of a Program permit being so revoked, Operator will not have an opportunity to reapply for a permit for at least one year.
- b) If Vehicle parking standards are not met on a monthly basis, the City reserves the right to revoke the Program permit.
- c) Grounds for terminating Program permits include, but are not necessarily limited to:
 - Failure to meet the terms and conditions set forth in the Program permit and/or the Rules and Guidelines;
 - Failure to put vehicles into service within 30 days;
 - Failure to share data;
 - Failure to abide by the MDS Specification;
 - Failure to abide by the LADOT MDS API Technical Compliance Overview v1.1 or any subsequent version
 - Failure to move vehicles located outside of the defined geo-fenced area.

Termination Payment

The City may terminate a Program permit issued without cause, in whole or in part, at any time by written notice to the Operators. Operators shall remit any final payment to the City no later than 60 days from the written notice of termination.

Waiver

The City's decision not to insist upon strict performance by the Operators of any provision of the permit in every one or more instances shall not constitute a waiver of such provision by the City, nor shall, as a result, the City relinquish any rights that it may have under the terms of the pilot program.

Liquidated Damages - Forfeiture

- a) As actual damages would be difficult, if not impossible to determine, the City and any Operator accepting permits under the Program agree that penalty for noncompliance with any provision of the Rules and Guidelines and other permit issuance requirements may result in termination of all or one Program permits, at the election of the City, without refund, reimbursement or adjustment or any and all fees paid to the City as of the date forfeiture for breach is determined. Determination shall be written notice from the City to the Operator.

Outreach & Equity

- a) Operators must attend meetings with City's Business Improvement Districts, Neighborhood Councils, Council Districts, surrounding municipalities, Transportation Management Organizations/Associations, Disability Rights Organizations/Centers for Independent Living, and any other community-based organization as stipulated by the City to introduce the Operators to them and make these communities aware of the Program and how it may affect the communities.
- b) Vehicles will be available at rates that are clearly and understandably communicated to the Customer prior to Vehicle use.
- c) Operators are responsible for educating the public on the Program, and on how to use the Vehicle safely.
- d) Operators are required to have a non-smart phone option for Customers to use the dockless Vehicle system.
- e) Operators are required to have a non-credit card option for Customers to use the dockless Vehicle system.
- f) Operators will offer a one-year low-income Customer plan that waives any applicable bicycle/e-scooter deposit and offers an affordable cash payment option and unlimited trips under 30 minutes to any customer with an income level at or below 200% of the federal poverty guidelines, subject to annual renewal.

Fees

Annual Permit Application Fees	\$20,000/year	Administration of the Permit. Fees shall be due upon application submittal (Non-Refundable)
Annual Vehicle Fee	\$130/vehicle per year	An increase in fleet size shall incur additional charges and must be paid prior to deployment.
Discounted	\$39/vehicle per	Discounts extend to vehicles deployed and maintained in

Vehicle Fee	year	CalEnviroScreen 3.0 Disadvantaged Communities. The discount represents a 70% reduction.
--------------------	------	---

- a) Applicants shall pay \$20,000 for an Annual Permit for the Program. Note if any stations or other structures are proposed, each site shall require additional review deposits and permitting.
- b) Applicants shall pay a program administrative fee of \$130/vehicle to the City.
- c) Any fees arising from the need for City crews to relocate or remove vehicles from any location where a vehicle is prohibited under this permit shall equal the Bureau of Sanitation’s Maintenance Laborer hourly rate plus any additional storage/impound fees.

6-Month Permit Extension*

6 Month Permit Application Fees	\$10,000	Administration of the Permit. Fees shall be due upon application submittal. (Non-Refundable)
6-Month Vehicle Fee	\$65/per vehicle	An increase in fleet size shall incur additional charges and must be paid prior to deployment.
6-Month Discounted Vehicle Fee	\$20/per vehicle	Discounts extend to vehicles deployed and maintained in CalEnviroScreen 3.0 Disadvantaged Communities. The discount represents a 70% reduction.

*Covers Program from 3/15/2020 -9/15/2020

Application Requirements

Permit applications must be succinct and all pages must be numbered. Boilerplate and glossy promotional materials are discouraged; any such materials deemed necessary should be included as a separate appendix and may or may not be considered as part of the evaluation. All components of the permit application shall be on 8.5" x 11" pages with the exception of two to three pages depicting imagery, mapping, etc. which may be on 11" x 17" pages. Font size shall be limited to 10-point font or larger with single line spacing.

Required Attachments including but not limited to:

- Completed DOCKLESS ON-DEMAND PERSONAL MOBILITY VERSION 0.2 PERMIT APPLICATION with signatures.
- Application agreement
- Synopsis of operator service model and qualifications, including images of the vehicles and mobile application
- Schedule for implementation, including the size of fleet and service area at launch
- Size and service area of any planned fleet expansions (optional)
- Organizational structure of operations team, including title, and their specific responsibilities on the project. There is a strong preference to hire locally.
- Screenshot illustrating how customers will be notified through a mobile and web application of the following:
 - Riders encouraged to wear helmets

- Riders must obey all traffic laws
- Proper parking procedures
- Operating an electric scooter on the sidewalk is prohibited
- Proof of general commercial liability insurance with a minimum liability limit of \$5,000,000 and that lists the “City of Los Angeles, its officers, agents and employees” as Primary additional insureds
- Proof of automobile insurance with limits of liability not less than One Million Dollars (\$1,000,000) and that lists the “City of Los Angeles, its officers, agents and employees” as Primary additional insureds.
- Proof of Workers' Compensation insurance as required by the State of California, with Statutory Limits and Employers' Liability Insurance with limits of no less than \$1,000,000 per accident for bodily injury or disease.
- Proof of umbrella insurance policy providing coverage in excess of its primary general liability, employer’s liability and automobile liability policies in an amount not less than \$5,000,000 per occurrence. The city of Los Angeles must be named as additional insured.
- Proof of performance bond of \$80/Vehicle.
- Indemnity Agreement (attachment provided by city).
- Permit application fee of \$10,000.
- 6-Month Vehicle fee of \$65/Vehicle.
- Organizational Chart & 24-Hour Contact Information
- Discounted Vehicle fee of \$20/vehicle for vehicles deployed and maintained in CalEnviroScreen 3.0 Disadvantaged Communities.

Modification of the Agreement

- a) The City may modify any of the terms and conditions contained in this Agreement at any time and in the City’s sole discretion.
- b) IF ANY MODIFICATION IS UNACCEPTABLE TO YOU, YOUR SOLE RECOURSE IS TO TERMINATE THIS AGREEMENT. YOUR CONTINUED USAGE OF THE SERVICES, SOFTWARE, AND/OR CONTENT FOLLOWING CITY’S MODIFICATION CONSTITUTES YOUR IRREVOCABLE AND BINDING ACCEPTANCE OF THE CHANGE.



LADOT Dockless Shared Mobility Program

MDS API Technical Compliance Overview

v1.1

March 4, 2020

Table of Contents:

- 1) Summary of Overall Approach
- 2) LADOT OMF MDS Agency API Workflows & Methodology
- 3) LADOT OMF MDS Agency API Compliance Overview
- 4) LADOT OMF MDS Agency API Technical Compliance
- 5) LADOT OMF MDS Agency API Technical Compliance Testing Methodology
- 6) LADOT OMF MDS Provider API Technical Compliance



1) Summary of Approach

This document defines MDS compliance through a set of tests and associated frequencies that facilitate initial and ongoing compliance assessments and operational audits of Mobility Service Providers (“MSP”) operating on the public right-of-way in the City of Los Angeles.

Overall compliance with LADOT’s Dockless Shared Mobility program is made up of two separate compliance measurements: technical compliance and operational compliance. **Technical compliance** refers to whether MSPs are properly providing the Open Mobility Foundation (OMF) MDS Provider endpoint, as well as interacting with the Los Angeles installation of the OMF MDS City Services API endpoints within rental and fleet management workflows. **Operational compliance** refers to how MSPs are performing against the LADOT set of equity, caps, and usage metrics.

Technical compliance consists of compliance to the OMF MDS Provider API, OMF MDS City Services API endpoints, and 311 Integration. This document specifically addresses Technical compliance with the Los Angeles installation of the OMF MDS City Services API endpoints along with the MSP-provided OMF MDS Provider endpoint.

How to use this document

This document identifies the compliance program that LADOT will use as part of managing the dockless mobility one year permit and any subsequent permit extension. This document should be treated as the authoritative source for compliance to: i) the Los Angeles installation of the OMF MDS City Services API endpoints; and ii) the Los Angeles requirements for MSP-provided OMF MDS Provider endpoint, and supersedes any previous documents.

This document does not outline how the City of Los Angeles shall enforce or remediate non-compliance issues with MSPs against permitting requirements.

References & Resources

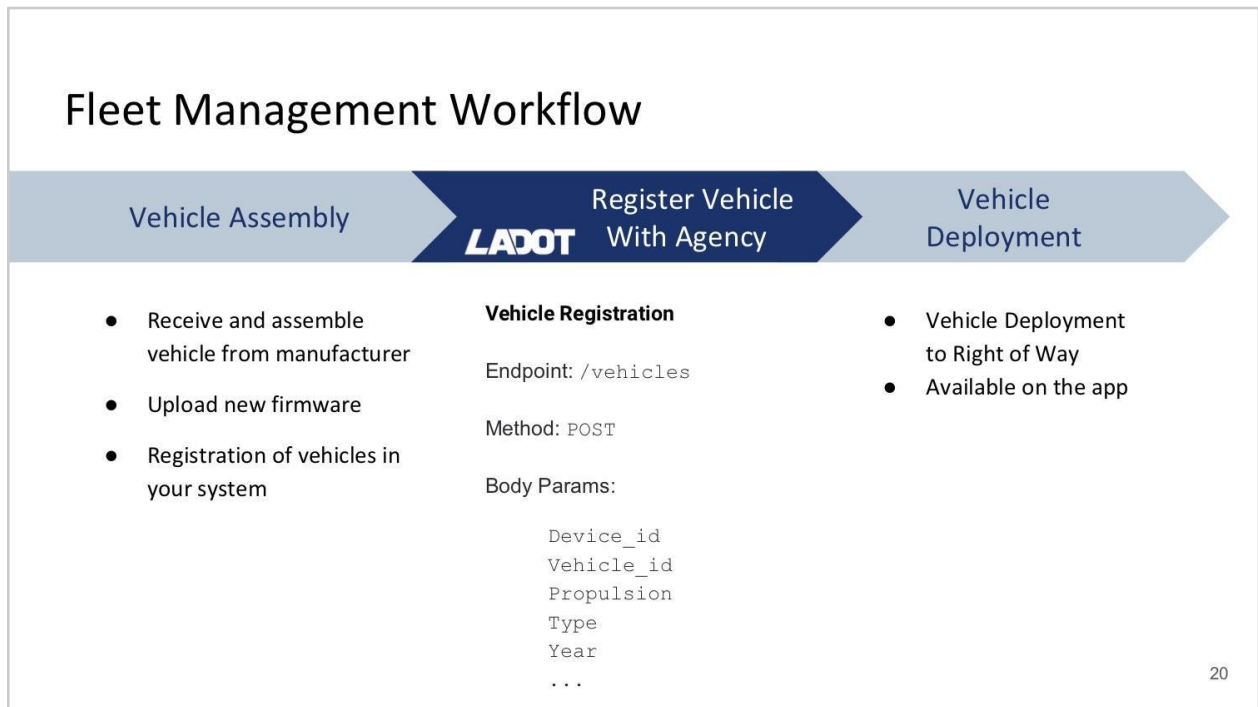
1. **MDS Github** - <https://github.com/CityOfLosAngeles/mobility-data-specification/>
2. **LADOT.io website** - <https://ladot.io/programs/dockless/>
3. **MDS Developer Webinar for One Year Permitting** - https://ladot.lacity.org/sites/g/files/wph266/f/MDS%20Developer%20Webinar%20-%20One%20Year%20Permitting%20Overview_03-06-19_REVISION.pdf
4. **Governing via API Open Source Collaboration in City Government** - <https://docs.google.com/presentation/d/1LekpQHM9JD5Is0JVqkL6jFn52r15e8hd7J2cquEJYVI/edit?usp=sharing>

2) LADOT OMF MDS City Services API Workflows & Methodology

Workflows and methodology are described in slides 20-26 of the LADOT **MDS Developer Webinar for One Year Permitting**, which are included below for easy reference. The full presentation can be found at the following weblink:

https://ladot.lacity.org/sites/g/files/wph266/f/MDS%20Developer%20Webinar%20-%20One%20Year%20Permitting%20Overview_03-06-19_REVISION.pdf

MDS Developer Webinar for One Year Permitting - Presentation Reference Slides



Deployment Workflow

Vehicle Deployment	LADOT Deploy Vehicle With Agency	Rental Operations
<ul style="list-style-type: none">• Vehicle Deployment to Right of Way	<p>Vehicle Event</p> <p>Endpoint: <code>/vehicles/{device_id}/event</code></p> <p>Method: <code>POST</code></p> <p>Body Params:</p> <pre>Event_type = 'service_start' rebalance_drop_off maintenance_drop_off</pre>	<ul style="list-style-type: none">• Start Service

21

Start Trip Workflow

Request Rental	LADOT Start Trip with Agency	Start Ride
<ul style="list-style-type: none">• User requests rental start• User scans barcode• Start of reservation	<p>Vehicle Event</p> <p>Endpoint: <code>/vehicles/{device_id}/event</code></p> <p>Method: <code>POST</code></p> <p>Body Params:</p> <pre>Event_type = 'trip_start'</pre>	<ul style="list-style-type: none">• Unlock Vehicle• Secure Payment• Notify App

22

Update Telemetry Workflow

End Ride OR $t \geq 30m$ OR $t \leq 24$ hrs



Update
Agency

End Ride OR $t < 24$ hrs after
End Ride

- During ride or after termination of ride

Telemetry

Endpoint:
`/vehicles/telemetry`

Method: `POST`

Body Params:

```
device_id  
timestamp  
GPS  
charge
```

- Prior to ride completion OR expiration of 24 hour period after ride.

End Trip Workflow

Start Ride || Update Telemetry



End Trip
With Agency

End Ride

- User requests rental start
- User scans barcode
- Start of reservation
- Update Telemetry

Vehicle Event

Endpoint:
`/vehicles/{device_id}/event`

Method: `POST`

Body Params:

`Event_type = 'trip_end'`

- Unlock Vehicle
- Secure Payment
- Notify App

25

Retrieval Workflow

Rental Operations



Retrieve Vehicle
With Agency

Removal

- Vehicle Deployment to Right of Way

Vehicle Event

Endpoint:
`/vehicles/{device_id}/event`

Method: `POST`

Body Params:

`Event_type = 'service_end'`

- Retrieval from street

26



3) LADOT OMF MDS City Services API Compliance Overview

Initial and Ongoing Compliance Goals

1. Verify that MSPs have correctly implemented support for the OMF MDS City Services API endpoints and continue that support through the permit program.
2. Make sure that Mobility Service Providers are accurately reporting data per the OMF MDS City Services API endpoints specification openmobilityfoundation.com/mobility-data-specification/agency and within the expected timing and behaviors outlined in this document.

Mobility Service Provider's Expectations

1. Integrate with LADOT's OMF MDS Agency APIs and notify LADOT of support prior to award of one-year permit and reaffirm support as part of any permit extension.
2. Use LADOT's OMF MDS Agency APIs for all vehicles in use on streets in the City of Los Angeles.
3. Submit all events accurately as described in the OMF MDS Agency specification.
4. Submit all events within the expected timing and behaviors outlined in this document.
5. Continue compliance with the OMF MDS Agency APIs over the duration of the one-year permit, including i) new versions of the mobile application you may release; ii) new versions of the OMF MDS Agency that LADOT may adopt; and iii) new timing and behaviors that LADOT may release.

4) MDS Agency API Technical Compliance

LADOT OMF MDS Agency API Initial Technical Compliance Stages

Initial verification of Technical compliance comprises three (3) stages that each MSP must pass through to earn the designation of technically compliant.

Stage 1- Not Compliant [State 0]

This is the default state of an MSP in the City of Los Angeles. This state is typically used when an MSP has not been tested or is in violation as a result of an operational or technical test.

Stage 2- In-Test [State 1]

This state is used to describe an MSP that is currently being tested by LADOT. Some testing requires a 24-36 hour period to complete.

Stage 3- Compliant [State 2]

This state is used to describe an MSP who has successfully passed all LADOT compliance testing.

Once an MSP has passed through the three stages outlined above, they are required to be in on-going Technical compliance with the LADOT OMF MDS City Services implementation. Ongoing Technical compliance with the LADOT OMF MDS Agency consists of the following:



LADOT OMF MDS Agency API On-going Technical Compliance Requirements

1. All dockless vehicles present in the LA public right-of-way (defined by /service_areas) must be registered with MDS registry endpoint (/vehicles) prior to deployment.
2. All vehicle events that involve public right-of-way must include accurate telemetry and timestamp, as described by the MDS event (/vehicles/{device_id}/event) endpoint.
3. Vehicles must have an associated *provider_drop_off* or *service_start* event posted (/vehicles/{device_id}/event) at the time the vehicle is placed in the public right-of-way.
4. All vehicles in the public right-of-way (/service_areas) and appearing in the MSP's app as available for rent must have a status of *available* in MDS and vice-versa.
5. Vehicles with a status of *available*, *unavailable*, *trip*, or *reserved* are considered in the public right-of-way and will count against vehicle caps.
6. Vehicles must have an associated *provider_pick_up* or *service_end* event posted (/vehicles/{device_id}/event) at the time the vehicle is removed from the public right-of-way.
7. Vehicles must have an associated *trip_enter* or *trip_leave* event posted (/vehicles/{device_id}/event) at the time a vehicle that is actively in use enters or leaves the LA city boundary (/service_areas).
8. Vehicles must have an associated (with trip_id) *trip_start* event posted (/vehicles/{device_id}/event) within 5 seconds of a user unlocking the vehicle for use.
9. Vehicles must have an associated (with trip_id) *trip_end* event posted (/vehicles/{device_id}/event) within 5 seconds of a user locking the vehicle via the MSP's mobile app.
10. Trip telemetry data must be provided via the telemetry endpoint (/vehicles/telemetry) during the trip or within 24 hours of trip completion. The telemetry data must include a telemetry measure point at least every 30 meters along the path traveled within the LA city boundary (/service_areas).
11. A *deregister* event should only be posted (/vehicles/{device_id}/event) when a vehicle is missing, with a high probability of not being recovered, or being taken out of service indefinitely.

5) MDS Agency API Technical Compliance - Testing Methodology

Technical compliance requires testing of the vehicle during normal operations including rental and maintenance workflows performed by the MSPs. Compliance is done in two parts. Part one is a Query testing using tooling that can be run from a desktop or that is automatically generated from a reporting engine built into the OMF MDS-core code. Part two is a set of in-field testing to assess compliance during rental operations. Either of these tests can be run using different types of tooling. The procedures for Query Testing and In-Field Testing are as follows:



Part One - Query Testing

1. For each MSP, ensure that > 250 vehicles are registered in the vehicle registry
2. For each MSP, ensure that > 250 vehicles are deployed in a relevant service area
3. For each MSP, ensure that >100 trips with Start Trip, End Trip and Telemetry have been recorded with Agency endpoints
4. For each MSP, ensure that there are >0 enter and leave events registered with Agency endpoints
5. For each MSP, ensure that there are >0 drop off events registered with Agency endpoints
6. For each MSP, ensure that /telemetry reporting was provided within 24 hours of end_trip event
7. For each MSP, ensure that /telemetry reporting was provided within 300 ft or 30 seconds of start_trip event

Part Two - In-Field Testing of a Mobility Service Provider

The in-field test is broken into two parts, a pre-rental test and post-rental test separated by a vehicle rental. These tests assess whether MSPs are accessing the LADOT OMF MDS Agency vehicle endpoints when prescribed. This test also has a delayed assessment for reporting trip telemetry data after 24 hours have elapsed.

Pre-Rental Procedure

1. Find a vehicle in the street to test according to a geography specific test plan outlined by the city.
2. Check to make sure that the vehicle is in the proper state by comparing the state of the vehicle on the ground against the state of the vehicle reported on the MDS compliance app and the Provider's app. Record any discrepancies on vehicle test report.
3. Scan QR code or enter the device_ID physically present on the vehicle into the MDS compliance app.

Vehicle Rental

1. Initiate process on MSP app to start a vehicle rental.
2. Ride vehicle for a period greater than 6 minutes and a distance greater than 1200 ft.
3. End rental using MSP application.

Post-Rental Procedure

1. Verify that the MSP properly notified LADOT of the scooter unlock using MDS compliance app.
2. Verify that the MSP properly notified LADOT of the scooter being locked using MDS compliance app.

24 our Post-Ride Procedure

1. Verify that the MSP notifies LADOT of the telemetry updates were reported on the compliance rides via the MDS compliance app. Record any exceptions.

6) LADOT OMF MDS Provider API Technical Compliance

MSPs must submit a pull request on GitHub (if they have not already received API compliance approval from LADOT), and submit the following OMF MDS Provider 0.4.1 API endpoint URLs (or any subsequent version as so directed by LADOT), either in a written attached document, or via email to ladot.innovation@lacity.org:

- MDS-Provider: trips
- MDS-Provider: status_changes
- MDS-Provider: Realtime Data, system_information
- MDS-Provider: Realtime Data, free_bike_status

Any MDS compatible API must expose data where:

- The trip starts in the City of Los Angeles, or
- The trip ends in the City of Los Angeles, or
- GPS telemetry data shows the trip passing through the City of Los Angeles, or
- A crow-flies path between trip start and trip end intersects the City of Los Angeles, or Shapefile of city boundaries on GeoHub located at: https://services5.arcgis.com/7nsPwEMP38bSkCjy/arcgis/rest/services/City_Boundary_geoJSON/FeatureServer

If MSP was previously approved for a conditional permit, the API endpoints should be production endpoints that reflect current operations. However, if MSP was not approved for the Conditional Permit, MSP may submit MDS compliant “Staging” URL endpoints with demonstration data. If MSP submits staging URL endpoints for the application, MSP must have production URLs verified by LADOT staff within one month of launch of operations.

A complete application must include a Mobility Data Specification (MDS) compliance confirmation from ladot.innovation@lacity.org. For questions about compliance with the data sharing requirements, please contact: ladot.innovation@lacity.org Attn: MDS in the subject line.

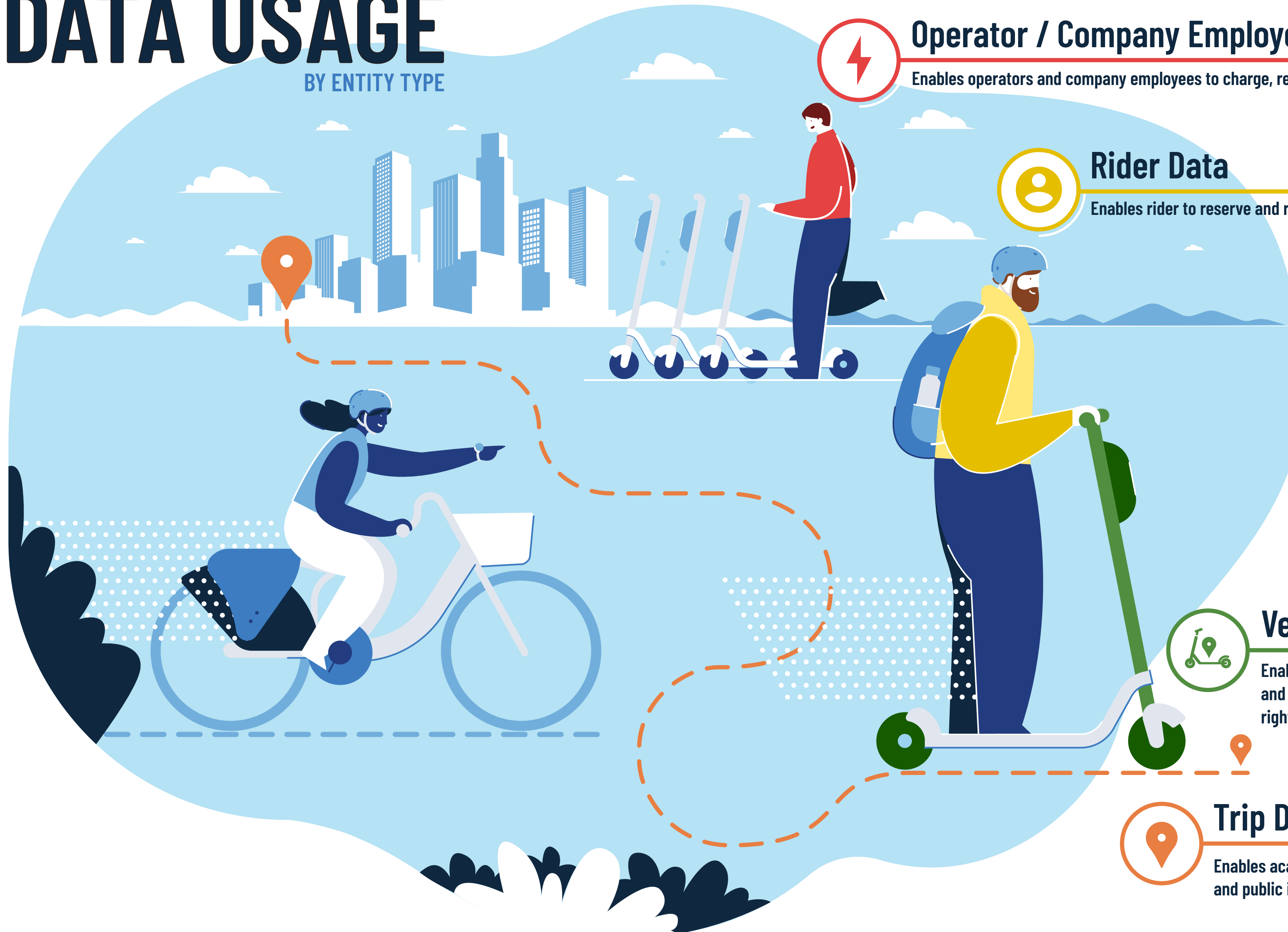
Date of Request	Requestor	Data Requested	Purpose	LADOT Response
February 2019	Academic or Research Institution	Dockless trip data	Multi-city study on shared urban mobility devices	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available
April 2019	Academic or Research Institution	Dockless vehicle availability, monthly by census block	Air pollution study	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available
May 2019	Government Transportation Planning Agency	general aggregate data of Mobility Data Specification if you have it available	Transportation Planning	Informed requestor LADOT would contact them when data sets are made publicly available
June 2019	Government Transportation Planning Agency	Raw trip data	First/Last Mile transportation planning projects	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available
July 2019	Academic or Research Institution	Dockless deployment and trip data	First/Last Mile and rideshare study	Informed requestor LADOT would contact them when data sets are made publicly available
July 2019	Private Service Provider or Company	Aggregated dockless data		Informed requestor LADOT would contact them when data sets are made publicly available
July 2019	Private Service Provider or Company	Monthly reports from permitted service providers		Records management informed them the data was confidential, we don't receive monthly reports
August 2019	Academic or Research Institution	MDS data and economic activity	Study on economic impacts of e-scooter services	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available
September 2019	Academic or Research Institution	Dockless trip origin/destination by census	Study on the built environment and socioeconomic influences on e-scooter use	Informed requestor LADOT would contact them when data sets are made publicly available
October 2019	Academic or Research Institution	Monthly data on dockless trips and total number of scooters in LA County	Study on e-scooters impacts on public transportation in LA County	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available
January 2020	Academic or Research Institution	Dockless ridership trends, trip miles	Study on medical records and scooter injuries	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available
January 2020	Non-profit Organization	Dockless deployment and trip data	Research	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available

Date of Request	Requestor	Data Requested	Purpose	LADOT Response
January 2020	Private Service Provider or Company	Dockless deployment data	Predict traffic patterns, site charging locations, and plan multimodal transit hubs.	Informed requestor data was confidential; LADOT would contact them when data sets are made publicly available
February 2020	Academic or Research Institution	MDS data on deployment and rebalancing in disadvantaged communities, trips taken using equity access options	Thesis research on dockless and equity	Answered general questions about pilot equity requirements; LADOT would contact them when data sets are made publicly available
February 2020	Media	Dockless deployment data		LADOT External Affairs provided monthly totals as previously reported to City Council
February 2020	Media	Dockless trip data by month, neighborhood, operator, vehicle type, trips per square mile per day, trips per day, service requests by neighborhood or Council District, average daily vehicles deployed in each area		LADOT informed them trip data was confidential, referred to LADOT Communications team
February 2020	Private Service Provider or Company	Monthly data reported by permitted providers		Informed requestor data was confidential

MDS Data Requests by Requestor Type	
Requestor Type	Total Requests
Academic or Research Institution	8
Private Service Provider or Company	4
Government Agency	2
Media	2
Non-Profit Organization	1
Law Enforcement Agency	0
Other	0
Total	17

DATA USAGE

BY ENTITY TYPE



Operator / Company Employee Data

Enables operators and company employees to charge, repair, manage vehicles

- Social Security Number
- Tax Information
- Bank Account



Rider Data

Enables rider to reserve and ride vehicles

- Full Name
- Home Address
- Cell Phone
- Email Address
- Credit Card
- Drivers License
- Birthdate
- Sex
- Height
- Weight
- Trip Costs
- Trip History
- Cell Phone GPS Location



Vehicle Data

Enables planning, regulation, and operations of public right-of-way

- Vehicle ID
- Trip Origin/Destination
- Trip Route
- Trip Duration
- Vehicle Status



Trip Data

Enables academic research and public insight

- Aggregated Trip Date
- Aggregated Trip Origin/Destination
- Aggregated Trip Duration

Company

Uses employee and rider data to employ personnel to manage their vehicle fleet, and enable riders to use their vehicles.

City

Uses vehicle data to identify right-of-way concerns, like having too many scooters in a particular area. City ensures trip data is de-identified before making it available for public use.