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

By: ____________________________________

Seleta J. Reynolds

General Manager

Department of Transportation

Date: __________________________________

[INSERT COMPANY NAME]

By: ____________________________________

Date: __________________________________

APPROVED AS TO FORM:

MICHAEL N. FEUER, City Attorney

By: ___________________________________

Date: _________________________________

By**: __________________________________

Title: __________________________________

Date: __________________________________