DRAFT

CITY DATA ADDENDUM

Mobile Parking Payment Systems for
Parking Management and Enforcement

Michael P. Ford
Parking & Mobility Division
Department of Transportation
City of Oakland
August 23, 2023

This City Data Addendum [”Addendum”] is Exhibit 1 to the Professional Services Agreement between the City of Oakland [“City”] and Contractor Name [“Contractor”] to provide Mobile Parking Payment Services [“Agreement”] as is set forth with specificity therein and is incorporated into the Agreement by this reference. In the event of a conflict between the terms and conditions of this Addendum and the Agreement, the terms of this Addendum shall prevail but only with respect to the matters stated herein.

1. Background

As is set forth with specificity in the Agreement's Statement of Work [Exhibit D], Contractor avers and covenants to develop, implement and operate a mobile parking payment system ["System"] that, at a minimum, will enable customers to remotely pay for parking sessions by using mobile phones or mobile devices to provide Contractor payment information which Contractor will collect and store for City on Contractor's mobile software application, website, and/or phone number for City-controlled paid parking ["Services"]. Contractor's Services may also support daily or monthly permits by zone merchant validation

Given the sensitive nature of the information Contractor will collect and store for City, Contractor further avers and covenants that its System and Services will meet the City's key goal of enhancing user data protections by complying with: (1) the City's Surveillance Technology Ordinance (Oakland Municipal Code Chapter 9.64); (2) the City's Surveillance Impact Report [Exhibit B]; and, (3) the City's Mobile Parking Payment Use Policy [Exhibit C], all of which are incorporated herein by this reference.

2. Scope and Ownership of Information to be Collected

The Agreement will require Contractor to collect from the users of its System, a broad range of personal and sensitive information. The California Consumer Privacy Act [CCPA][1] and Consumer Privacy Rights Act ["CPRA"] [2] definitions for "personal information"[3] and "sensitive personal information"[4] are incorporated herein by this reference and shall apply to the information Contractor collects.

[1] Cal. Civ. Code Section 1798 *et. seq.*

[2] The CPRA is more accurately described as an amendment of the CCPA. The CPRA specifically states that it "amends" existing provisions of Title 1.81.5 of the California Civil Code (currently known as the CCPA) and "adds" new provisions (related to the establishment of the California Privacy Protection Agency).

[3] It identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.

[4] It contains some or all of the following;

- social security, driver's license, state identification card, or passport number
- account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account.

With the exception of that information which is publicly known or available as set forth in Section 5 [“Confidential Information”] of the Agreement, City data [“Data”] shall consist of any and all data disclosed or provided by the City to Contractor, including but not limited to, all data, files, documentation, information, communications, media, whether intangible or tangible, whether provided directly or indirectly by Contractor to provide its Services, together with any and all results of Contractor’s providing of its Services, including all data Contractor accesses, collects, modifies, develops as work product, or otherwise generates while providing its Services to City under this Agreement, whether pursuant or incidental to the purposes of the Agreement and whether or not delivered to the City, shall be the exclusive property of, and all ownership rights therein shall vest in, the City (collectively “City Data”).

To the extent necessary, Contractor hereby assigns to the City, the rights to City Data which arise out of, or are developed in connection with or are the results of, Contractor’s Services.

3. Use of City Data

3.1 By Contractor

Contractor avers and covenants to:

- Comply with the terms of the City’s Surveillance Technology Ordinance [OMC 9.64]
- Comply with
  - the City’s Surveillance Impact Report [Exhibit B];
  - the City’s Mobile Parking Payment Use Policy [Exhibit C],
- Anonymize the City Data and take such other steps as may be required to assure that personally identifiable or personally sensitive information are not visible to City staff at any time for any reason;

- Not sell, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate orally, in writing, or by electronic or other means, City Data, to another business or a third party for monetary or other valuable consideration;
- Only share City Data with third parties as permitted by City's Mobile Parking Payment Use Policy [Exhibit C; Section 8 "Third-Party Data-Sharing"];
- Only use City Data to fulfill its obligations to City under the Agreement;
- Comply with the terms of the Agreement;
- Implement security safeguards;
- Not combine City Data with personal information received from others;
- Notify City when it uses subcontractors;
- Pass through the Agreement's terms and conditions to any subcontractors it uses;

.

Notwithstanding any other law or provision of this Agreement, Contractor shall, during its provision of Services to City as called for hereunder, take all steps necessary to assure that all Data resulting from its Services is kept confidential and disclosed: (1) only to Contractor's personnel, agents or subcontractors with an absolute need to have access to the Data, who have executed a Confidentiality Agreement with Contractor sufficient to enable Contractor to comply with the requirements of this Section 4, with Contractor remaining liable for any breach of this Section 4 by its personnel, agents or subcontractors; and (2) to the City Project Manager for such dissemination as the City Project Manager, in its sole discretion, determines should be made; or (3) as required by law

Contractor shall fully indemnify City for any third-party claims against City resulting from Contractor's use of City Data in violation of this Addendum's provisions.

3.2 By City

City's access to City Data shall be limited to authorized staff and used only as permitted by City's Surveillance Use Policy [Exhibit B] and as required by City's parking enforcement responsibilities [Resolution 84664 C.M.S.] which include but, are not limited to, shaping parking policies and practices to better support the City's Parking Principles and developing a more equitable mobility system. In this regard, only designated DOT and Finance Department staff will have access through unique portal credentials to the following *anonymized* City Data Contractor stores:

- Estimating parking demand, occupancy, and revenues;
- Evaluating parking payment options;
- Monitoring demand-responsive parking areas and compliance;
- Reconciling payment transactions with total parking revenues received;
- Promoting compliance and enforcing parking restrictions, permits, and payment;
- Reviewing contested parking citations;
- Remitting user transaction fees to Providers via invoices;

4. Contractor's System Security

This Agreement requires Contractor to store City Data in Contractor's certified data center[s] which are external to the City's premises and administered by Contractor for the purposes of this Agreement ["System"]. City's Data is highly sensitive, confidential and is of paramount importance to the City because unauthorized disclosures of the Data could seriously harm the City and possibly third parties.

Contractor acknowledges that City, in entering into this Agreement with Contractor, is relying upon Contractor's professional expertise, know-how, judgment, experience and its representations in its System Security Plan that the integrity of the security, availability and processing of its System protects and preserves the confidentiality and privacy of the City Data. Contractor warrants that its System has been accredited under industry recognized standards [e.g., SOC 2] and that, at all times, Contractor will maintain and ensure that the Data remains secure and does not through any of Contractor's actions or lack of action thereof become vulnerable to unauthorized access by third parties.

Contractor avers and covenants to continue to take all technical and organizational measures necessary to protect the information technology systems and data used in connection with the operation of the Contractor's business. Without limiting the foregoing, Contractor will continue to use reasonable efforts to establish and maintain, implement and comply with, reasonable information technology, information security, cyber security and data protection controls, policies and procedures, including oversight, access controls, encryption, technological and physical safeguards and business continuity/disaster recovery and security plans that are designed to protect against and prevent breach, destruction, loss, unauthorized distribution, use, access, disablement, misappropriation or modification, or other compromise or misuse of or relating to any information technology system or data used in connection with the operation of Contractor's business.

Contractor agrees to maintain the City Data and to not disclose such information except as required to perform hereunder or as required by law. Contractor shall maintain network risk and cyber liability coverage (including coverage for unauthorized access, failure of security, breach of privacy perils, as well at notification costs and regulatory defense) as required by the City's Schedule Q. Such insurance shall be maintained in force at all times during the term of this Agreement.

Notwithstanding as may be otherwise provided in either this Addendum or this Agreement and, with the exception of those instances for which the City is responsible, Contractor avers and covenants to be solely responsible for restoring and correcting any corruption to City's Data that occur by reason of Contractor's actions or lack thereof, including ransomware attacks upon Contractor and to fully indemnify the City for any claims against City and injury to City resulting from corruptions of the City Data.

5. DATA INCIDENTS

a. Contractor shall implement and maintain a program for managing unauthorized disclosures of, access to, or use of City Data however they may occur (“Data Incident”). In case of a Data Incident, or if Contractor knows or reasonably suspects a Data Incident has occurred, Contractor shall:

(i) Promptly, and in any case in a manner to ensure notice within 24 hours, notify City’s Director of Information Technology/Chief Information Office and Chief Security Officer, or their designees of the Data Incident or suspected Data Incident;

(ii) Cooperate with City and law enforcement agencies, where applicable, to investigate and resolve the Data Incident, including without limitation by providing reasonable assistance to City in notifying injured third parties; and

(iii) Otherwise comply with applicable laws governing data breach notification and response.

b. In case of a Data Incident or reasonably suspected Data Incident, Contractor shall, upon request by City:

(i) immediately conduct a reasonable investigation of the reasons for and circumstances surrounding such Data Incident or reasonably suspected Data Incident;

(ii) use best efforts and take all necessary actions to prevent, contain, and mitigate the impact of, such Data Incident or reasonably suspected Data Incident;

(iii) collect and preserve all evidence concerning the discovery, cause, vulnerability, remedial actions and impact related to such Data Incident or reasonably suspected Data Incident, which shall meet reasonable expectations of forensic admissibility; and

(iv) document the incident response and remedial actions taken in detail, which shall meet reasonable expectations of forensic admissibility.

c. In addition, if the Data Incident results from Contractor’s breach of this Agreement or negligent or unauthorized act or omission, including without limitation those of its subcontractors or other agents, Contractor shall:

(i) Indemnify City for any reasonable expense related to notification of consumers;

(ii) Provide 2 years of credit monitoring service to any affected individual.

(iii) Contractor shall give City prompt access to such records related to a Data Incident as City may reasonably request. City will treat such records as Contractor’s Confidential Information pursuant to Section 122 below [“Proprietary or Confidential Information]. Contractor is not required to give City access to records that might compromise the security of Contractor’s other customers.

City will coordinate with Contractor on the content of any intended public statements or required notices for the affected individuals and/or notices to the relevant authorities regarding the Data Incident.

6. Termination of the Agreement

Within ten (10) days of the date of termination of the Agreement for any reason, Contractor shall send all City Data to City in a format acceptable to the City and which protects and preserves the sensitive nature of the City Data. Contractor may not keep copies of the City Data. For the purposes of this provision, Contractor’s Assignment of the Agreement under Section 10 [“Assignment”] or Bankruptcy under Section 33 [“Bankruptcy”] of the Agreement or cessation of business shall be considered a Termination of the Agreement.