

PROPOSED AMENDMENT

Master Services Agreement between Flock Group, Inc. and the City of Ridgecrest

Sections 4.3 and 5.3, with conforming amendments

Purpose

This document proposes replacement language for Sections 4.3 and 5.3 of the Master Services Agreement dated March 21, 2024, together with the conforming amendments necessary to give those sections effect.

Each item sets out the existing text, the basis for the change, and the proposed replacement. Provisions are drafted so that each may be evaluated independently.

Section 11.7 (Special Terms) provides that mutually executed special terms control over conflicting language in the Agreement. The Parties may wish to adopt these provisions as Special Terms rather than restating the Agreement in full.

Summary of our group's objectives

1. Rights in data collected on the City's behalf end when the Agreement ends. Neither Section 4.3 nor Section 5.3 survives termination.
2. Disclosure occurs only on a defined, externally verifiable standard, with notice to the City.
3. No data collected on the City's streets reaches any federal agency or any agency outside California in any capacity.
4. The City can see who queries its data, and that visibility cannot be reduced without the City's approval.
5. Anonymization is a documented and independently verified practice rather than an assertion.
6. Material changes to the Agreement or to system configuration require approval by the Ridgecrest City Council.

Item 1 — Section 4.3 (Anonymized Data)

Existing text

4.3 Anonymized Data. Flock shall have the right to collect, analyze, and anonymize Customer Data and Customer Generated Data to the extent such anonymization renders the data non-identifiable to create Anonymized Data to use and perform the Services and related systems

and technologies, including the training of machine learning algorithms. Customer hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right to use and distribute such Anonymized Data to improve and enhance the Services and for other development, diagnostic and corrective purposes, and other Flock offerings. Parties understand that the aforementioned license is required for continuity of Services. Flock does not own and shall not sell Anonymized Data.

Basis for the amendment

The license granted is perpetual and is not limited to the Services the City purchases. Section 4 is omitted from the survival provision at Section 7.3, leaving the effect of termination unresolved. The closing sentence commits only that Flock will not sell the data, while the operative grant is a **right to “use and distribute” it**; the commitment therefore does not reach the conduct the grant permits.

Proposed replacement

4.3 Derived Data. Flock shall have the right to collect, analyze, and anonymize Customer Data and Customer Generated Data solely as necessary to provide the Services to Customer during the Term.

(a) Definition. “Derived Data” means any data generated from, extracted from, or based upon Customer Data or Customer Generated Data, including without limitation anonymized, aggregated, de-identified, hashed, statistical, synthetic, embedded, vectorized, or model-derived outputs, and any model weights or parameters trained on such data.

(b) License grant. Customer grants Flock a non-exclusive, royalty-free, non-transferable, revocable license to use Derived Data solely to provide, maintain, and support the Services to Customer, and solely during the Term.

(c) Prohibited uses. Flock shall not use, distribute, license, sell, transfer, disclose, or otherwise commercialize Customer Data, Customer Generated Data, or Derived Data for: (i) training, tuning, or evaluating machine learning or artificial intelligence models; (ii) developing, improving, or marketing any product or service other than the Services provided to Customer under this Agreement; (iii) any other Flock offering; or (iv) provision to any third party.

(d) No sale or distribution. Flock does not own and shall not sell, distribute, license, or transfer Customer Data, Customer Generated Data, or Derived Data.

(e) Effect of termination. All rights granted under this Section terminate automatically upon expiration or termination of this Agreement. No license granted under this Section survives termination. Within thirty (30) days of termination, Flock shall delete or irreversibly destroy all Customer Data, Customer Generated Data, and Derived Data in its possession or control, including in backups and archives, and shall provide Customer written certification of such destruction signed by an officer of Flock.

(f) Application to prior data. This Section applies to all Customer Data, Customer Generated Data, and Derived Data collected at any time, including data collected prior to the effective date of this amendment.

(g) Confirmation of compliance. Upon reasonable notice, and no more than twice annually, Customer may request written confirmation of Flock's compliance with this Section, including a description of all uses of Derived Data during the preceding period.

Item 2 — Section 4.3 anonymization methodology

Basis for the amendment

Section 1.1 defines Anonymized Data as data “permanently stripped of identifying details and any potential personally identifiable information, by commercially available standards which irreversibly alters data in such a way that a data subject ... can no longer be identified directly or indirectly.” Section 4.3 authorizes anonymization only “to the extent such anonymization renders the data non-identifiable.” The two provisions state different standards, and neither identifies the method applied or how compliance is demonstrated.

The City is presently required to accept the adequacy of anonymization as an assertion. A general security attestation does not address anonymization methodology and is not responsive to this concern.

Proposed new subsection

(h) Anonymization standard and documentation. Data shall not be treated as Anonymized Data unless it satisfies the standard set forth in Section 1.1, including the requirement that a data subject can no longer be identified directly or indirectly. Flock shall provide Customer, upon written request and no less than annually, documentation of the anonymization methodology applied, including:

- (i) each data field removed, generalized, aggregated, hashed, or otherwise altered;
- (ii) the technique applied and the parameters used, including any generalization, suppression, aggregation, perturbation, or noise-addition thresholds;
- (iii) the methodology by which Flock assesses the risk of indirect re-identification, including re-identification of a data subject through the combination of location, timestamp, and vehicle attribute data; and
- (iv) validation of the foregoing by a qualified independent third party engaged for that purpose.

For the avoidance of doubt, a SOC 2 attestation, ISO certification, or other general information security attestation does not satisfy subsection (iv). Flock bears the burden of demonstrating that any data treated as Anonymized Data satisfies Section 1.1.

Item 3 — Section 5.3 (Disclosure of Footage)

Existing text

5.3 Disclosure of Footage. Subject to and during the Retention Period, Flock may access, use, preserve and/or disclose the Footage to law enforcement authorities, government officials, and/or third parties, if legally required to do so or if Flock has a good faith belief that such access, use, preservation or disclosure is reasonably necessary to comply with a legal process, enforce this Agreement, or detect, prevent or otherwise address security, privacy, fraud or technical issues, or emergency situations.

Basis for the amendment

The Section permits disclosure on a standard applied by Flock to itself, to categories of recipients the Agreement does not define, with no obligation to notify the City that a disclosure has occurred. The City is subject to California Civil Code section 1798.90.55, which provides that a public agency shall not sell, share, or transfer automated license plate reader information except to another public agency and only as otherwise permitted by law. Ridgecrest Police Department Policy 427.7 states that such data is not permitted to be shared with any agency outside California.

The City acknowledges that this Section is bounded by the thirty (30) day Retention Period and does not concern a permanent archive. The City's objection is to unreviewable discretion, not to the duration of storage.

Proposed replacement

5.3 Disclosure of Footage.

(a) Definitions. For purposes of this Section:

(i) "California Law Enforcement Agency" means a police department, sheriff's office, district attorney, or other public agency of the State of California or of a political subdivision of the State of California whose primary function is the enforcement of California criminal law. The term expressly excludes any agency, department, bureau, task force, or instrumentality of the United States government; any agency of any other state, territory, or tribal government; any foreign government or agency thereof; and any private entity.

(ii) "Authorized Government Official" means an officer or employee of Customer, or of a California Law Enforcement Agency, acting within the scope of official duties and identified to Customer in advance in writing. The term expressly excludes any officer or employee of the United States government, and excludes any officer serving on a federal task force or acting in a federally deputized capacity, when acting in that capacity.

(iii) The term “third parties” is struck. Flock shall make no disclosure to any person or entity other than Customer, a California Law Enforcement Agency, or an Authorized Government Official, except as required by subsection (c)(iii).

(b) Federal and out-of-state disclosure prohibited. Flock shall not disclose, transfer, sell, share, make available, provide access to, or permit any query of Footage or Customer Data by any federal agency, federal task force, officer acting in a federally deputized capacity, agency of any other state, tribal agency, or foreign government, whether directly, indirectly, through a shared or interconnected network, through a search or lookup interface, through an integration or application programming interface, or by any other means. This prohibition applies without regard to any request, agreement, or arrangement between Flock and any such entity, and applies to Derived Data.

(c) Permitted disclosures. Flock shall not access, use, preserve, or disclose Footage or Customer Data except:

- (i) as strictly necessary to provide the Services to Customer;
- (ii) upon Customer’s prior written authorization identifying the recipient and the data;
- (iii) as compelled by a warrant, subpoena, court order, or other binding legal process issued by a court of competent jurisdiction, subject to subsections (d) and (e); or
- (iv) where necessary to prevent imminent death or serious bodily injury, subject to subsection (f).

(d) Notice before disclosure and right to object. Prior to disclosing Footage or Customer Data pursuant to subsection (c)(iii), Flock shall provide Customer written notice and a reasonable opportunity, of not less than five (5) business days where circumstances permit, to object or to seek a protective order, unless notice is prohibited by the terms of the legal process itself. Where notice is prohibited, Flock shall provide notice as soon as the prohibition lapses. Flock shall not voluntarily comply with any request that is not compulsory legal process.

(e) Minimization. Any disclosure under subsection (c)(iii) shall be limited to the specific records described in the legal process and shall not include bulk data, historical query results, or Derived Data.

(f) Emergency disclosures. A disclosure under subsection (c)(iv) requires that Flock have a specific and articulable factual basis, documented in writing at the time of disclosure, that disclosure is necessary to prevent imminent death or serious bodily injury to an identified person. Such disclosure shall be limited to the minimum data necessary and shall be made only to a California Law Enforcement Agency or an emergency medical or fire service. Flock shall notify Customer in writing within twenty-four (24) hours, providing the contemporaneous documentation. A general concern regarding security, privacy, fraud, or technical operation does not constitute an emergency under this subsection.

(g) Notice after disclosure. Flock shall notify Customer in writing within seventy-two (72) hours of any disclosure under this Section, identifying the recipient, the data disclosed, the date and time of disclosure, and the legal basis or emergency circumstance relied upon.

(h) Records of disclosure. Flock shall maintain a record of every disclosure made under this Section, shall make that record available to Customer on demand and in the quarterly reporting described in Item 4, and shall retain such records for no less than two (2) years notwithstanding the Retention Period. Customer may publish such records.

(i) No survival. This Section does not survive expiration or termination of this Agreement. Following termination, Flock shall hold no Footage or Customer Data, as provided in Item 6.

Item 4 — Access by parties other than Customer; audit records

Basis for the amendment

Section 1.8 defines “Flock Network End User” but the Agreement does not otherwise govern enrollment in sharing networks or provide the City visibility into queries run against its data by parties other than its own Authorized End Users. Records presently available to the City do not identify the organization associated with an external query. California Civil Code section 1798.90.52 requires records of access to include the username and, as applicable, the organization or entity with whom the person accessing is affiliated, together with the purpose for the access. Regulatory audits in other jurisdictions have examined whether vendor-side controls are adequate to ensure compliance with state-specific sharing restrictions. The City requires visibility sufficient to verify compliance directly rather than relying on assurances.

Proposed new Section

(a) Network enrollment. Customer shall not be enrolled in, and Flock shall not enable, any regional, statewide, national, or inter-agency sharing, lookup, or search network without Customer’s prior written authorization identifying each participating agency. Flock shall not enroll Customer in any such network by default, by product update, or by configuration change.

(b) Roster of access. Flock shall provide Customer, upon request and no less than quarterly, a complete list of every Flock Network End User, agency, vendor, contractor, subprocessor, and other entity with any form of access to Customer Data, identifying the entity, the nature of the access, and the date access was granted.

(c) External query logging. Flock shall provide Customer, no less than quarterly, a complete log of all queries run against Customer Data by any party other than Customer’s Authorized End Users, identifying the querying agency or entity, the querying user, the date and time, the data elements used to query, and the stated purpose. Customer may publish this log.

(d) Content of audit records. Audit records available to Customer shall include, at minimum: the date and time of access; the data elements used to query the system; the username of the person accessing and the organization or entity with which that person is affiliated; and the purpose for the access.

(e) No reduction of audit information. Flock shall not reduce, redact, remove, obscure, aggregate, or eliminate any field, record, category, or capability of the audit log or the transparency reporting made available to Customer without Customer's prior written approval. Any change to audit logging shall require sixty (60) days' prior written notice and Customer's written approval, and Flock shall on request identify the party that requested any such change.

(f) Quarterly reporting. Flock shall provide Customer quarterly reporting summarizing all access to and disclosure of Customer Data, including all disclosures under Section 5.3 and all external queries under subsection (c). Customer may publish such reporting.

Item 5 — Section 2.4 (Upgrades to Platform); material changes

Basis for the amendment

Section 2.4 permits Flock to make platform changes it deems necessary or useful, provided they do not materially change the terms of the Agreement, with Flock determining what is material. Certain configuration settings determine data retention, sharing, and the content of audit records. The City requires that changes affecting those functions, and material changes to the Agreement itself, receive the approval of its governing body.

Proposed addition

(a) No upgrade, modification, or configuration change shall reduce, redact, or eliminate any field, record, or capability of the audit log; alter data retention periods; alter sharing or network participation defaults; enable any new data-sharing relationship; or add automated analytic, facial recognition, or artificial intelligence features, without Customer's prior written approval. Flock shall provide Customer sixty (60) days' written notice of any change affecting data handling, retention, sharing, or logging.

(b) No material change to this Agreement, to any Order Form, or to any terms of service, privacy policy, acceptable use policy, or product terms incorporated by reference shall take effect without the prior written approval of the Ridgecrest City Council given at a public meeting. Material changes include any change to provisions governing data ownership, licensing, permitted uses, retention, sharing, disclosure, audit logging, or security.

(c) Flock shall not modify any term of this Agreement by unilateral amendment, by notice, by continued use, or by reference to any externally hosted document.

Item 6 — Sections 7.1, 7.2 and 7.3 (Term, Termination, Survival)

Existing text of Section 7.3

7.3 Survival. The following Sections will survive termination: 1, 3, 5, 6, 7, 8.3, 8.4, 9, 11.1 and 11.6.

Basis for the amendment

Section 4 is not included in the survival provision, while Section 4.3 grants a license described as perpetual and Section 4.1 grants a license described as irrevocable. Section 5 is included, with the result that the disclosure provision continues to operate after termination. Section 7.2 provides for removal of hardware upon termination but does not address the disposition of data. The City proposes resolving each of these expressly.

The City further requires that renewal be an affirmative act of its governing body rather than an automatic consequence of inaction.

Proposed replacement of Section 7.1

7.1 Term. The initial term of this Agreement shall be as set forth on the Order Form (the “Term”). This Agreement shall not renew automatically. Any renewal requires the affirmative written agreement of both Parties, and on Customer’s part requires approval by the Ridgecrest City Council at a public meeting prior to the expiration of the then-current Term. Flock shall provide Customer written notice of the approaching expiration, together with any proposed changes to fees or terms, no less than one hundred twenty (120) days prior to the end of the then-current Term. If no renewal is approved, this Agreement expires at the end of the then-current Term without further action by either Party.

Proposed addition to Section 7.2

Upon expiration or termination of this Agreement, Flock shall cease all collection of Customer Data, shall disable all Flock Hardware deployed for Customer, and shall return or irreversibly destroy all Customer Data, Customer Generated Data, and Derived Data in its possession or control, including in backups and archives, and shall provide Customer written certification of such destruction signed by an officer of Flock within thirty (30) days. Any data Flock proposes to retain following termination shall be specifically enumerated in a writing executed by both Parties identifying the data, the purpose of retention, the duration of retention, and the legal authority relied upon. Flock shall make no disclosure of Customer Data following termination except as compelled by binding legal process, and shall notify Customer of any such disclosure within seventy-two (72) hours.

Proposed replacement of Section 7.3

7.3 Survival. The following Sections will survive termination: 1, 3, 5.1, 5.2, 6, 7, 8.3, 8.4, 9, 11.1 and 11.6. For the avoidance of doubt, no provision of Section 4 and no provision of Section 5.3 survives expiration or termination of this Agreement, and no license granted under Section 4 shall be construed as perpetual or irrevocable following termination.

Item 7 — Section 4.1 (Customer Data) and Section 4.2 (Customer Generated Data)

Existing text of Section 4.1

4.1 Customer Data. As between Flock and Customer, all right, title and interest in the Customer Data, belong to and are retained solely by Customer. Customer hereby grants to Flock a limited, non-exclusive, royalty-free, irrevocable, worldwide license to use the Customer Data and perform all acts as may be necessary for Flock to provide the Flock Services to Customer. Flock does not own and shall not sell Customer Data.

Basis for the amendment

The license granted in Section 4.1 is described as irrevocable while being limited to acts necessary to provide the Services. Because the Services end upon termination, the City proposes conforming the duration of the license to the purpose for which it is granted. The closing commitment in Sections 4.1 and 4.2 addresses sale only, and does not reach distribution or transfer.

Proposed amendments

- (a) In Section 4.1, strike “irrevocable” and insert at the end of the second sentence: “which license terminates upon expiration or termination of this Agreement.”
- (b) In Sections 4.1 and 4.2, replace “Flock does not own and shall not sell” with “Flock does not own and shall not sell, distribute, license, or transfer.”

Summary of items

Item 1 — Section 4.3 replaced; license limited to the Term and to provision of the Services; no survival.

Item 2 — Anonymization methodology documented and independently validated; general security attestations do not satisfy the requirement.

Item 3 — Section 5.3 replaced; “third parties” struck; recipients defined; federal and out-of-state disclosure prohibited; notice and right to object; no survival.

Item 4 — Network enrollment requires authorization; external queries logged and reported quarterly; audit information may not be reduced without approval.

Item 5 — Configuration and material contract changes require Council approval.

Item 6 — No automatic renewal; data destroyed and certified on termination; survival provision corrected.

Item 7 — Section 4.1 license conformed to its purpose; no-sale commitments extended to distribution and transfer.

We welcome discussion of alternative language that accomplishes these objectives.