DATA PROCESSING AGREEMENT

Version 2.0 | March 2026

Kvadrat Systems L.L.C

PREAMBLE

This Data Processing Agreement ("**DPA**") forms an integral part of and supplements the service agreement, commercial offer, statement of work, or other principal agreement ("**Principal Agreement**") between **Kvadrat Systems L.L.C** ("**Processor**"), a limited liability company incorporated in Dubai, United Arab Emirates (Trade License No. 674763, TDRA Certificate No. DA35806/14), registered at Business Bay, P.O. Box 27795, Dubai, UAE, and the entity identified in the Principal Agreement ("**Controller**" or "**Client**").

This DPA governs the processing of Personal Data by the Processor on behalf of the Controller in connection with the Services, ensuring compliance with: (a) the UAE Personal Data Protection Law (Federal Decree-Law No. 45 of 2021 and its Executive Regulations, "**UAE PDPL**"); (b) the EU General Data Protection Regulation (Regulation (EU) 2016/679, "**GDPR**"), where applicable to the processing of Personal Data of EU/EEA data subjects; (c) the California Consumer Privacy Act as amended by the CPRA ("**CCPA**"), where applicable; and (d) all other applicable data protection and privacy laws (collectively, "**Data Protection Laws**").

WHEREAS the Processor provides IoT/GPS tracking, vehicle tracking, asset management, security systems, and related technology services that may involve the processing of precise geolocation data, device telemetry, and other categories of Personal Data on behalf of the Controller;

NOW THEREFORE, the Parties agree to the terms set forth herein.

1. DEFINITIONS

"Approved Sub-processor" means a Sub-processor listed in Annex B or subsequently approved by the Controller in accordance with Section 5.

"Controller" means the entity that determines the purposes and means of Processing of Personal Data, as identified in the Principal Agreement.

"Data Protection Laws" means the UAE PDPL, GDPR (where applicable), CCPA (where applicable), and all other applicable data protection, privacy, and electronic communications laws.

"Data Subject" means an identified or identifiable natural person to whom Personal Data relates.

"EEA" means the European Economic Area (EU Member States plus Iceland, Liechtenstein, and Norway).

"Personal Data" means any information relating to a Data Subject that is Processed by the Processor in connection with the Services, including but not limited to precise geolocation data (GPS coordinates), device identifiers, and telemetry data.

"Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored, or otherwise Processed.

"Processing" (and cognates) means any operation or set of operations performed on Personal Data, whether or not by automated means, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

"Processor" means Kvadrat Systems L.L.C, which Processes Personal Data on behalf of the Controller.

"SCCs" means the Standard Contractual Clauses for the transfer of Personal Data to processors in third countries, as approved by European Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

"Services" means the services described in the Principal Agreement, including IoT/GPS tracking platforms, vehicle tracking systems, asset management solutions, BLE/RFID systems, security systems, software (web/mobile/API), and related professional services.

"Sub-processor" means any third party (excluding employees of the Processor) engaged by the Processor to Process Personal Data on behalf of the Controller.

"Supervisory Authority" means the UAE Data Office, an EU/EEA data protection authority, or any other competent authority responsible for monitoring compliance with Data Protection Laws.

"Technical and Organizational Measures" or "TOMs" means the security measures described in Annex A, as updated from time to time.

2. SCOPE AND DETAILS OF PROCESSING

2.1 Processing Pursuant to Instructions

The Processor shall Process Personal Data solely on and in accordance with the Controller's documented instructions as set forth in this DPA and the Principal Agreement, unless required to do so by applicable law to which the Processor is subject. In such event, the Processor shall inform the Controller of that legal requirement before Processing, unless the law prohibits such notification on important grounds of public interest. The Processor shall immediately inform the Controller if, in the Processor's opinion, an instruction infringes Data Protection Laws.

2.2 Details of Processing

Element	Description
Subject Matter	Provision of IoT/GPS tracking, vehicle tracking, asset management, BLE/RFID, security systems, and related technology services as described in the Principal Agreement.
Duration	The term of the Principal Agreement, plus the period necessary for data return and/or deletion in accordance with Section 8.
Nature of Processing	Collection, storage, organization, structuring, retrieval, consultation, use, disclosure by transmission to Controller, alignment, restriction, erasure, and destruction.
Purpose of Processing	Service delivery (real-time tracking, alerts, reporting), account management, technical support, hardware fulfillment, anonymized analytics, and compliance with legal obligations.
Categories of Data Subjects	Controller's employees; authorized drivers/operators; end-users of Controller's services; business contacts; fleet managers; any other individuals whose data Controller submits through the Services.
Categories of Personal Data	Identity data (names, employee/driver IDs); contact data (email, phone, address); account credentials; device data (GPS coordinates, speed, heading, altitude, IMEI, serial numbers, firmware versions); telemetry (ignition, fuel, OBD/CAN-bus data where applicable); usage data (login timestamps, API calls); financial data (billing info).
Sensitive/Special Category Data	Precise geolocation data (GPS coordinates) which may constitute sensitive data under certain jurisdictions. No other special categories (health, biometric, racial, etc.) are intentionally Processed unless explicitly agreed in writing.

3. OBLIGATIONS OF THE PROCESSOR

3.1 Confidentiality (GDPR Art. 28(3)(b); UAE PDPL)

The Processor shall ensure that all persons authorized to Process Personal Data:

- Have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Have received mandatory data protection and information security training before being granted access to Personal Data, with refresher training conducted at least annually;
- Process Personal Data only in accordance with the Controller's instructions and the terms of this DPA.

3.2 Security of Processing (GDPR Art. 28(3)(c), Art. 32; UAE PDPL Art. 29)

The Processor shall implement and maintain the Technical and Organizational Measures set forth in **Annex A**, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of Processing, as well as the risks to the rights and freedoms of Data Subjects. The Processor shall regularly test, assess, and evaluate the effectiveness of these measures.

The Processor shall not materially decrease the overall level of security during the term of this DPA. Any material changes to the TOMs shall be notified to the Controller in writing at least thirty (30) days in advance.

3.3 Assistance with Data Subject Rights (GDPR Art. 28(3)(e); UAE PDPL)

The Processor shall, taking into account the nature of the Processing, assist the Controller by appropriate technical and organizational measures in fulfilling the Controller's obligations to respond to Data Subject requests, including rights of access, rectification, erasure, restriction, portability, and objection. The Processor shall:

- Promptly notify the Controller (within **forty-eight (48) hours**) if the Processor receives a request directly from a Data Subject, without responding to that request unless expressly authorized by the Controller or required by law;
- Provide the Controller with all cooperation, information, and technical capabilities necessary to fulfill Data Subject requests within the timelines mandated by applicable Data Protection Laws (30 days under GDPR; as specified under UAE PDPL);
- Implement and maintain technical mechanisms that enable the Controller to retrieve, correct, delete, or export Personal Data in a structured, commonly used, machine-readable format upon request.

3.4 Assistance with Compliance (GDPR Art. 28(3)(f))

The Processor shall assist the Controller in ensuring compliance with its obligations under Data Protection Laws, including with respect to: (a) data protection impact assessments (DPIAs); (b) prior consultation with Supervisory Authorities; (c) security of Processing; (d) notification of Personal Data Breaches; and (e) maintenance of records of Processing activities (Article 30 GDPR). Such assistance shall be provided taking into account the nature of Processing and the information available to the Processor.

4. PERSONAL DATA BREACH NOTIFICATION

4.1 Notification Obligation

The Processor shall notify the Controller of any confirmed or reasonably suspected Personal Data Breach **without undue delay and in no event later than forty-eight (48) hours** after the Processor becomes aware of such breach. The notification shall include, to the extent then available:

- A description of the nature of the breach, including (where possible) the categories and approximate number of Data Subjects and Personal Data records affected;
- The name and contact details of the Processor's designated data protection contact;
- A description of the likely consequences of the breach;
- A description of the measures taken or proposed to address the breach, including measures to mitigate its possible adverse effects;
- Any other information necessary for the Controller to fulfill its breach notification obligations to Supervisory Authorities (within 72 hours under GDPR Art. 33) and to affected Data Subjects (GDPR Art. 34; UAE PDPL).

4.2 Cooperation and Remediation

The Processor shall: (a) cooperate fully with the Controller in investigating, remediating, and mitigating the breach; (b) preserve all relevant evidence and logs; (c) not make any public statement regarding the breach without the Controller's prior written consent (unless required by law); and (d) provide ongoing updates to the Controller as additional information becomes available.

4.3 Record-Keeping

The Processor shall maintain a register of all Personal Data Breaches, including their circumstances, effects, and the remedial actions taken, regardless of whether such breaches are reportable to Supervisory Authorities. This register shall be made available to the Controller upon request.

5. SUB-PROCESSORS (GDPR Art. 28(2), (4))

5.1 General Authorization

The Controller grants the Processor a **general written authorization** to engage Sub-processors for the Processing of Personal Data, subject to the requirements of this Section 5. The list of current Approved Sub-processors as of the Effective Date is set forth in **Annex B**.

5.2 New Sub-processors

The Processor shall notify the Controller in writing at least **thirty (30) days** prior to engaging any new Sub-processor or replacing an existing Sub-processor. Such notice shall include the identity, registered address, country of processing, and a description of the Processing activities to be performed by the proposed Sub-processor.

5.3 Controller's Right to Object

The Controller may object to the engagement of a new Sub-processor on **reasonable, documented grounds** relating to data protection within **fifteen (15) days** of receiving the notice. If the Controller objects:

- The Processor shall use commercially reasonable efforts to make available an alternative solution that avoids the use of the objected-to Sub-processor;
- If no alternative is reasonably available within thirty (30) days, either Party may terminate the affected Services (and only those Services) upon written notice, without penalty;
- The Processor shall not engage the objected-to Sub-processor for the Controller's data until the objection is resolved.

5.4 Sub-processor Agreements

The Processor shall impose on each Sub-processor, by way of a binding written agreement, data protection obligations that are **no less protective** than those set out in this DPA, including confidentiality obligations, security requirements, and restrictions on further sub-processing. The Processor shall remain **fully liable** to the Controller for the performance of each Sub-processor's obligations as if such obligations were performed by the Processor itself.

6. AUDIT AND INSPECTION RIGHTS (GDPR Art. 28(3)(h))

6.1 Information and Documentation

The Processor shall make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA and Article 28 of the GDPR, including: (a) copies of relevant certifications (SOC 2 Type II, ISO 27001, or equivalent); (b) summaries of penetration test results and security assessments; and (c) records of Processing activities (Article 30 GDPR).

6.2 On-site and Remote Audits

The Controller (or a qualified, independent third-party auditor appointed by the Controller and bound by confidentiality) shall have the right to conduct audits, including on-site inspections, to verify compliance with this DPA, subject to the following conditions:

- The Controller shall provide at least **thirty (30) days** prior written notice (except in the case of an audit required following a Personal Data Breach or by a Supervisory Authority, in which case reasonable notice shall be sufficient);
- Audits shall be conducted during normal business hours, with minimal disruption to the Processor's operations;
- Audits shall be limited to **once per calendar year**, unless a Personal Data Breach has occurred or a Supervisory Authority requires or requests an audit;
- The Processor shall cooperate fully and provide reasonable access to relevant premises, systems, personnel, and records;
- Audit findings shall be treated as Confidential Information of the Processor.

6.3 Sub-processor Audits

The Controller's audit rights extend to the Processing activities of Sub-processors. The Processor shall use commercially reasonable efforts to facilitate such audits, either directly or by obtaining and providing to the Controller relevant audit reports or certifications from its Sub-processors.

7. INTERNATIONAL DATA TRANSFERS

7.1 General Restriction

The Processor shall not transfer Personal Data to any country or territory outside: (a) the United Arab Emirates; or (b) the EEA (where applicable), without the prior written consent of the Controller and unless appropriate safeguards are in place as required by applicable Data Protection Laws.

7.2 Transfer Mechanisms

Permitted transfer mechanisms include:

- **Adequacy Decisions:** Transfers to countries recognized as providing an adequate level of protection by the European Commission, UAE authorities, or other competent body;
- **Standard Contractual Clauses:** Where the Controller is established in the EEA and data is transferred to the UAE or another third country, the Parties agree that the EU SCCs (Commission Implementing Decision (EU) 2021/914) are hereby incorporated by reference, with **Module Two (Controller to Processor)** applying. The Annexes to the SCCs shall be populated with the information in Section 2.2 and Annex A of this DPA;
- **Binding Corporate Rules:** Where applicable and approved by competent Supervisory Authorities;
- **Supplementary Measures:** Where required by the Schrems II guidance (EDPB Recommendations 01/2020), the Processor shall implement additional technical, organizational, and contractual measures to ensure the effectiveness of the transfer mechanism.

7.3 UAE PDPL Cross-Border Transfers

For transfers subject to the UAE PDPL, the Processor shall ensure compliance with any cross-border data transfer requirements imposed by the UAE Data Office, including obtaining the Controller's explicit consent and ensuring that the recipient country provides an adequate level of protection or that appropriate safeguards are in place.

8. DATA RETURN AND DELETION (GDPR Art. 28(3)(g))

8.1 Upon Termination

Upon termination or expiration of the Principal Agreement, or upon the Controller's earlier written request, the Processor shall, at the Controller's election:

- **Return** all Personal Data to the Controller in a structured, commonly used, machine-readable format (CSV, JSON, or other format reasonably requested by the Controller) within **thirty (30) days** of receiving the Controller's written instruction; and/or

- **Securely delete** all Personal Data, including all copies, replicas, and backups, within **sixty (60) days** of termination, using methods that render recovery infeasible (e.g., cryptographic erasure, NIST SP 800-88 compliant methods).

8.2 Certification of Deletion

The Processor shall provide the Controller with **written certification of deletion** within ten (10) business days of completing the deletion process, signed by an authorized officer of the Processor.

8.3 Legal Retention

Where applicable law requires the Processor to retain certain Personal Data beyond the termination date, the Processor shall: (a) notify the Controller of such requirement, specifying the relevant legal basis and the data concerned; (b) isolate the retained data from other Processing; (c) apply the TOMs to the retained data; and (d) Process such data only to the extent required by the applicable legal obligation.

9. LIABILITY AND INDEMNIFICATION

9.1 Limitation of Liability

SUBJECT TO SECTION 9.3, EACH PARTY'S TOTAL AGGREGATE LIABILITY TO THE OTHER PARTY ARISING OUT OF OR IN CONNECTION WITH THIS DPA (WHETHER IN CONTRACT, TORT, STRICT LIABILITY, OR OTHERWISE) SHALL NOT EXCEED THE **TOTAL FEES PAID OR PAYABLE BY THE CONTROLLER TO THE PROCESSOR UNDER THE PRINCIPAL AGREEMENT IN THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE EVENT GIVING RISE TO THE CLAIM**.

9.2 Exclusion of Indirect Damages

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NEITHER PARTY SHALL BE LIABLE TO THE OTHER FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES, INCLUDING BUT NOT LIMITED TO LOSS OF PROFITS, LOSS OF REVENUE, LOSS OF DATA (BEYOND THE COST OF REASONABLE DATA RECOVERY), LOSS OF BUSINESS, BUSINESS INTERRUPTION, LOSS OF GOODWILL, OR VEHICLE DOWNTIME, ARISING OUT OF OR IN CONNECTION WITH THIS DPA, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

9.3 Exceptions to Liability Limitations

The limitations in Sections 9.1 and 9.2 shall **not** apply to:

- Liability arising from a Party's **gross negligence, willful misconduct, or fraud**;
- Liability for **death or personal injury** caused by negligence;
- The Controller's **payment obligations** under the Principal Agreement;
- Regulatory **fines and penalties** imposed directly on a Party by a Supervisory Authority for that Party's own breach of Data Protection Laws (each Party bears its own fines).

9.4 Mutual Indemnification

Processor Indemnification: The Processor shall indemnify, defend, and hold harmless the Controller against all third-party claims, damages, losses, costs, and expenses (including reasonable legal fees) arising from the Processor's breach of this DPA or applicable Data Protection Laws, except to the extent such claim arises from the Controller's instructions, actions, or failure to comply with its own obligations.

Controller Indemnification: The Controller shall indemnify, defend, and hold harmless the Processor against all third-party claims, damages, losses, costs, and expenses (including reasonable legal fees) arising from: (a) the Controller's breach of its obligations under this DPA or Data Protection Laws; (b) the Controller's instructions that infringe Data Protection Laws (provided the Processor has notified the Controller of such infringement); or (c) the Controller's collection, use, or disclosure of Personal Data in a manner not authorized by this DPA or applicable law.

10. OBLIGATIONS OF THE CONTROLLER

- The Controller shall ensure that Personal Data is collected, used, and disclosed in accordance with applicable Data Protection Laws, including obtaining all necessary consents, authorizations, and providing required notices to Data Subjects.
- The Controller shall provide clear, lawful, documented instructions for the Processing of Personal Data and shall ensure that such instructions do not require the Processor to violate Data Protection Laws.
- The Controller shall promptly notify the Processor of any changes to applicable Data Protection Laws or regulatory guidance that materially affect the Processor's obligations.
- The Controller shall be solely responsible for the accuracy, quality, and legality of the Personal Data and the means by which it was collected.
- The Controller warrants that it has a lawful basis for all Processing instructions and that the Processing contemplated by this DPA does not violate any applicable law.

- The Controller shall cooperate with the Processor in connection with Data Subject requests, Supervisory Authority inquiries, and data breach investigations.

11. TERM AND TERMINATION

This DPA shall remain in effect for the duration of the Principal Agreement and for as long as the Processor retains any Personal Data on behalf of the Controller. Sections 3.1 (Confidentiality), 4 (Breach Notification), 8 (Data Return/Deletion), 9 (Liability and Indemnification), and 12 (General Provisions) shall survive termination or expiration.

The Controller may terminate this DPA immediately by written notice if the Processor: (a) materially breaches this DPA and fails to cure such breach within thirty (30) days of written notice; (b) persistently fails to comply with a binding decision of a competent Supervisory Authority; or (c) enters insolvency proceedings.

12. GENERAL PROVISIONS

12.1 Governing Law. This DPA shall be governed by and construed in accordance with the laws of the United Arab Emirates as applied in the Emirate of Dubai. To the extent that mandatory provisions of GDPR, UAE PDPL, CCPA, or other applicable Data Protection Laws apply, such mandatory provisions shall take precedence.

12.2 Dispute Resolution. Any dispute arising out of or in connection with this DPA shall be resolved in accordance with the dispute resolution provisions of the Principal Agreement. In the absence of such provisions, disputes shall be submitted to the exclusive jurisdiction of the courts of Dubai, UAE, or, at the election of either Party, to binding arbitration at the Dubai International Arbitration Centre (DIAC).

12.3 Conflict. In the event of conflict: (a) between this DPA and the Principal Agreement, this DPA shall prevail with respect to the Processing and protection of Personal Data; (b) between this DPA and the EU SCCs (where applicable), the SCCs shall prevail.

12.4 Severability. If any provision of this DPA is held to be invalid, illegal, or unenforceable, the remaining provisions shall continue in full force and effect. The Parties shall negotiate in good faith to replace any invalid provision with a valid provision that achieves substantially the same commercial and legal intent.

12.5 Entire Agreement. This DPA, together with the Principal Agreement, applicable SCCs, and the Annexes hereto, constitutes the entire agreement between the Parties with respect to the Processing of Personal Data and supersedes all prior agreements, discussions, and understandings relating to such subject matter.

12.6 No Waiver. The failure of either Party to enforce any right or provision of this DPA shall not constitute a waiver of such right or provision. Any waiver must be in writing and signed by the waiving Party.

12.7 Amendments. No amendment to this DPA shall be effective unless made in writing and signed by authorized representatives of both Parties. The Processor may update Annex A (TOMs) from time to time to reflect improvements in security measures, provided that the overall level of protection is not materially decreased.

12.8 Notices. All notices under this DPA shall be in writing and sent to the addresses specified in the Principal Agreement, or by email to: Processor: legal@kvadratsystems.com / dpo@kvadratsystems.com; Controller: as specified in the Principal Agreement.

SIGNATURES

IN WITNESS WHEREOF, the Parties have executed this Data Processing Agreement as of the date last signed below.

CONTROLLER (Client)		**PROCESSOR (Kvadrat Systems L.L.C)**
Signature: ________________________		Signature: ________________________
Name: ____________________________		Name: ____________________________
Title: ______________________________		Title: ______________________________
Date: ______________________________		Date: ______________________________

ANNEX A: TECHNICAL AND ORGANIZATIONAL MEASURES

The following measures represent the minimum security standards maintained by the Processor. The Processor may exceed these standards at any time.

Category	Measure	Details
Encryption	Data at rest	AES-256 encryption for all stored Personal Data, including databases and backups.
Encryption	Data in transit	TLS 1.2+ (TLS 1.3 preferred) for all data transmitted over public networks. Certificate pinning for mobile applications.
Access Control	Authentication	Multi-factor authentication (MFA) mandatory for all administrative and privileged access. Strong password policies enforced.
Access Control	Authorization	Role-based access control (RBAC) with principle of least privilege. Segregation of duties for critical operations.
Access Control	Access reviews	Quarterly access reviews. Immediate revocation upon termination of personnel.
Network Security	Perimeter	Next-generation firewalls, intrusion detection/prevention systems (IDS/IPS), DDoS protection.
Network Security	Segmentation	Network segmentation isolating production, staging, and development environments.
Monitoring	Logging	Centralized logging of all access to Personal Data with tamper-evident log storage. Minimum 12-month log retention.
Monitoring	SIEM	Security Information and Event Management (SIEM) with 24/7 alerting for anomalous activity.
Physical Security	Data centers	Tier III+ data centers with biometric access, CCTV surveillance, environmental controls.
Business Continuity	Backups	Automated daily backups with encryption. Geographic redundancy. Regular restoration testing.
Business Continuity	DR plan	Documented disaster recovery plan. RTO: 4 hours; RPO: 1 hour.
Incident Response	Plan	Documented incident response plan with defined roles, escalation matrix, and communication protocols. Tested annually.
Personnel	Background checks	Background verification for all personnel with access to Personal Data.
Personnel	Training	Mandatory annual data protection and security awareness training. Phishing simulations.
Vulnerability Mgmt	Testing	Annual penetration testing by independent third party. Quarterly vulnerability scanning. Patch management within SLA.
Data Minimization	Retention	Automated data lifecycle management. Data retained only as long as necessary for the specified purpose.

ANNEX B: APPROVED SUB-PROCESSORS

The following Sub-processors are authorized as of the Effective Date. This list shall be updated in accordance with Section 5 of this DPA.

Sub-processor	Country	Processing Activity	Data Categories
[Cloud Hosting Provider]	[Country]	Infrastructure hosting; data storage and compute	All categories as described in Section 2.2
[Payment Processor]	[Country]	Payment processing	Financial data (billing information)
[Email/Communications]	[Country]	Transactional email delivery	Contact data (email addresses)
[Analytics Provider]	[Country]	Anonymized usage analytics	Usage data (anonymized)
[To be completed prior to execution]			

End of Data Processing Agreement v2.0 | Kvadrat Systems L.L.C | Business Bay, P.O. Box 27795, Dubai, UAE
This document should be reviewed by qualified legal counsel before execution.