

ORIGIN DATA LAB

Website & Field Operations Policy

Public Policy for Website Use, Managed Field Collection, Privacy Handling, Operator Safety, and Dataset Governance

VERSION	LAST UPDATED	DOCUMENT TYPE
1.1	July 16, 2026	Public Policy

Important: This document provides general public and operational information. Project-specific rights, obligations, pricing, licensing, delivery, privacy, retention, and data-processing terms are defined in the applicable campaign terms, proposal, statement of work, license, or commercial agreement.

Company: OriginDataLab Co., Ltd.
Website: <https://origindatalab.io> | Email: contact@origindatalab.io

1. Introduction

This Website & Field Operations Policy explains the public operating principles applied by Origin Data Lab to website use, managed field collection, submitted recordings and metadata, operational safety, privacy handling, operator compensation rules, licensing boundaries, and related data-governance activities.

It is intended to provide general information to website visitors, approved field operators, customers, and procurement teams. It is not a project-specific agreement and does not replace any applicable campaign terms, proposal, statement of work, data-processing terms, license, or commercial agreement.

2. Scope

This policy applies to the Origin Data Lab website, approved field-collection workflows, and the operational systems used to receive, review, manage, and prepare field data.

- Website inquiries and communications submitted to Origin Data Lab.
- Participation by approved field operators in managed collection missions.
- Submitted video, images, audio where applicable, sensor data, metadata, and supporting operational records.
- Technical validation, quality review, privacy handling, acceptance, rejection, and delivery-preparation workflows.
- General safety, compensation, licensing, and usage-boundary rules.

Additional requirements may apply to a specific collection campaign or customer engagement and will be documented separately where appropriate.

3. Information and Data We Collect

Depending on the interaction, collection mission, and technical workflow, Origin Data Lab may collect and process information including:

- Contact and communication information submitted through the website, email, or other approved contact channels.
- Field-operator account and device information, including device model, operating-system version, application version, and assigned operator identifiers.
- Location, GPS, route, timing, and mission-related information where required for collection operations.
- Video recordings, images, audio where enabled, sensor readings, timestamps, and related capture metadata.
- Upload status, validation results, delivery history, quality-review outcomes, technical logs, and other operational records.
- Website analytics and diagnostic information collected through Google Analytics 4 and related website technologies to understand page usage, traffic sources, visitor activity, and website performance.

The specific information collected depends on the applicable website interaction, assigned collection mission, project scope, device capabilities, and operational requirements.

4. Purposes of Processing and Use

Information and submitted field data may be processed for purposes including:

- Managing website inquiries, business communications, support requests, procurement discussions, and customer qualification.
- Administering approved field-collection missions, operator participation, delivery tracking, and compensation review.
- Performing upload verification, technical validation, quality control, privacy review, provenance tracking, and dataset preparation.
- Producing custom datasets for model training, evaluation, validation, benchmarking, research, and other approved machine-learning workflows.
- Preparing, licensing, and delivering datasets under an applicable customer agreement or approved delivery scope.
- Maintaining records for security, fraud prevention, dispute handling, audit support, and legal or contractual requirements.
- Understanding website performance and visitor activity through analytics and diagnostic information.

Origin Data Lab does not collect field data for the purpose of identifying, tracking, profiling, or targeting specific individuals. Use of delivered datasets remains subject to the applicable agreement, approved scope, and customer responsibilities.

Origin Data Lab currently uses Google Analytics 4, a third-party analytics service provided by Google, to understand website traffic and usage patterns. Google may process related technical and usage information according to its own privacy terms.

5. Customer Delivery and Service-Provider Access

Dataset materials may be provided to approved customers, research partners, service providers, professional advisers, infrastructure providers, or other parties where access is required for an authorized operational, technical, contractual, or legal purpose.

Customer deliveries may include processed video, images, metadata, sensor information, labels, manifests, quality documentation, or other project-specific materials according to the approved delivery scope.

Access and delivery are subject to applicable contractual and operational controls, which may include restrictions on redistribution, resale, sublicensing, public release, unauthorized disclosure, re-identification, and use outside the approved project or license scope.

Origin Data Lab may use service providers to support hosting, storage, communications, analytics, technical operations, payment processing, or professional services. Access is limited to the functions required for the relevant service or engagement.

6. Privacy Processing and Identifying Elements

Field data may contain faces, license plates, signs, addresses, voices, location details, or other elements that could directly or indirectly relate to an identifiable person or location.

Privacy-processing requirements are determined according to the applicable collection mission, project scope, delivery specification, contractual terms, and legal requirements. Controls may include:

- Face detection, masking, blurring, exclusion, or human-in-the-loop review where required by the approved project specification.
- License-plate detection, masking, blurring, exclusion, or human-in-the-loop review where required by the approved project specification.
- Filtering or restricting address details, private-location indicators, or other identifying visual information.
- Excluding or restricting sensitive, review-flagged, or unsuitable scenes.
- Limiting access to raw or unprocessed materials.

Origin Data Lab does not represent that every submitted recording is automatically or completely anonymized. Privacy processing applied to a customer delivery is defined before delivery through the approved project specification, contractual requirements, and delivery documentation.

7. Legal and Operational Grounds for Processing

The grounds and conditions for processing information vary according to the type of information, the collection region, the relationship with the relevant person, and the purpose of the workflow. Depending on the circumstances and applicable law, processing may be supported by:

- Consent or acknowledgment provided by an approved field operator for account, device, location, capture, upload, and participation activities.
- Contractual necessity for managing collection missions, field-data delivery, compensation, customer projects, and related communications.
- Legitimate operational or business interests, where permitted by applicable law and balanced against relevant rights and risks.
- Compliance with legal, regulatory, security, audit, dispute-resolution, or contractual obligations.
- Other lawful grounds that may apply to a specific jurisdiction, project, or processing activity.

Field-operator consent or acknowledgment does not represent consent from people, drivers, passengers, or other individuals who may incidentally appear in recordings captured in publicly accessible environments.

8. Publicly Accessible Environment Data

Managed field collection may take place on publicly accessible roads, in markets, traffic environments, transport areas, and other urban settings. Recordings may incidentally include people, vehicles, storefronts, signs, buildings, and other elements present in those environments.

Collection missions are intended to capture general environmental, mobility, traffic, infrastructure, and scene context rather than to identify, monitor, or target a specific individual.

Field operators must follow applicable mission instructions, safety rules, restricted-location rules, and local operational requirements. Recordings that intentionally target individuals, private activities, prohibited areas, or unsuitable sensitive content may be rejected, restricted, or removed from the workflow.

9. Cross-Border Handling and International Transfers

Information and dataset materials may be collected, uploaded, stored, reviewed, processed, or delivered across more than one country depending on the collection region, infrastructure, service providers, customer location, project team, and approved delivery scope.

Where a processing activity involves a regulated international transfer of personal data, the relevant legal, contractual, security, and operational requirements will be identified according to the applicable engagement and jurisdiction.

Origin Data Lab does not claim that a single transfer mechanism or legal framework applies to every collection mission or customer engagement.

10. Data Retention

Information and field data are retained only for defined operational, technical, quality-control, security, contractual, legal, audit, and delivery-related purposes.

Retention periods may vary according to:

- The category and sensitivity of the information.
- The collection mission or customer project.
- Quality review, provenance, fraud-prevention, and traceability requirements.
- Whether the data has been accepted, rejected, delivered, restricted, or placed under additional review.
- Legal, contractual, dispute-resolution, security, payment, or audit obligations.
- Backup, recovery, and technical deletion cycles.

Raw footage is not retained solely because it exists. Retention decisions are based on defined operational and project requirements, subject to applicable internal controls and legal obligations.

11. Rights and Requests

Depending on applicable law and a person's relationship with Origin Data Lab, an individual may have rights concerning personal information, including access, correction, deletion, restriction, objection, or portability.

Requests may be submitted through the contact channels published on the Origin Data Lab website or through an approved operational channel. A request may require verification of identity, operator account, field-data delivery, device, mission, date, location, or other information reasonably necessary to locate and assess relevant records.

Requests are reviewed according to applicable law, technical feasibility, security requirements, existing customer deliveries, contractual obligations, and the rights of other parties.

12. Deletion Requests and Limitations

Approved field operators and other eligible individuals may request deletion or restriction of relevant personal information where such rights apply.

Where a request is valid and the relevant data can be reasonably identified, Origin Data Lab may take steps including:

- Deleting or restricting relevant account, contact, device, location, field-data delivery, or raw-data records from active systems.

- Restricting future internal use of identifiable source materials.
- Updating operational records to reflect the request and review outcome.
- Contacting relevant service providers or recipients where required, appropriate, and technically practicable.

Deletion may be limited where:

- The requested data cannot be reliably identified from the information provided.
- The material has already been irreversibly anonymized or aggregated.
- The material has been incorporated into an existing delivered dataset, customer workflow, backup, archive, or trained model.
- Retention is necessary for legal, contractual, security, audit, fraud-prevention, compensation, or dispute-resolution purposes.
- Deletion would adversely affect the rights, security, or lawful interests of another party.

Where relevant data has been transferred to a customer's independently controlled systems, models, backups, or other environments, retrieval, restriction, or removal from those environments is subject to the customer's technical capabilities, legal obligations, and applicable contractual responsibilities.

13. Security and Access Controls

Origin Data Lab applies technical and organizational controls intended to reduce unauthorized access, loss, misuse, alteration, or disclosure of information and dataset materials. Controls may include:

- Access restrictions based on assigned operational roles and project needs.
- Controlled cloud-based storage and upload workflows.
- Authentication, permission, and account-management controls.
- Technical validation, field-data delivery tracking, and operational logging.
- Restricted handling of raw footage, identifying information, and review-flagged materials.
- Secure transmission or encryption capabilities where supported by the relevant infrastructure and workflow.
- Backup, recovery, operational review of security-relevant events, and access-revocation procedures according to operational requirements.

No technical or organizational system can guarantee absolute security. Security controls may differ according to the project, infrastructure, data category, service provider, and approved delivery requirements.

14. Field-Data Acceptance, Rejection, and Operator Compensation

Delivery of a recording or related field data does not guarantee acceptance, inclusion in a dataset, or operator compensation.

Field data may be rejected, excluded, restricted, removed, or treated as ineligible for compensation where it:

- Fails applicable technical, quality, duration, format, metadata, device, or upload requirements.
- Does not follow the assigned collection mission or recording instructions.
- Contains duplicate, manipulated, misleading, fabricated, incomplete, or fraudulent material.
- Intentionally targets individuals or private activities.
- Includes prohibited, unsafe, restricted, or unsuitable sensitive content.
- Was captured in violation of safety rules, local restrictions, platform rules, or applicable law.
- Cannot be verified, traced, reviewed, or matched to an approved field operator or mission.

Origin Data Lab may use automated checks, technical validation, quality review, human review, metadata analysis, fraud controls, and operational records when determining acceptance or rejection.

Where operator compensation is offered, eligibility, review timing, payment amount, payment method, acceptance criteria, and any available review or dispute process are defined in the applicable collection campaign, operator instructions, agreement, or other approved operational terms.

15. Field-Operator Safety

Safety takes priority over completing a collection mission. Field operators must not capture data in a manner that creates danger, distraction, collision risk, unlawful conduct, confrontation, or unreasonable interference with other people.

Field operators must not:

- Operate a recording device unsafely while driving or controlling a vehicle.
- Enter restricted, private, dangerous, police, military, or otherwise prohibited areas.
- Obstruct traffic, pedestrians, emergency operations, or public access.
- Intentionally follow, confront, provoke, or target an individual.
- Intentionally center a recording on an identifiable minor or other vulnerable individual unless the activity is specifically authorized, lawful, and subject to appropriate project controls.
- Continue recording when instructed by an authorized person to stop where such instruction is legally valid and applicable.
- Continue a mission during dangerous weather, crowd conditions, civil disturbance, or other circumstances that make responsible capture impracticable.
- Complete a mission where the operator cannot do so safely and lawfully.

A field operator should stop or abandon a mission where environmental, legal, technical, or safety conditions make responsible capture impracticable.

16. Dataset Licensing and Usage Boundaries

Dataset materials are provided only under the applicable proposal, license agreement, statement of work, order, or approved delivery documentation.

The applicable agreement defines authorized use, organizational scope, delivery rights, restrictions, ownership arrangements, exclusivity where applicable, and rights relating to derived materials, annotations, trained models, or other project outputs.

Unless expressly authorized in writing, recipients may not redistribute, resell, sublicense, publicly release, or use dataset materials outside the approved scope. Recipients must not attempt to identify or re-identify individuals appearing in the data or use the materials for unlawful surveillance, targeting, harassment, discrimination, or other prohibited purposes.

Binding rights, obligations, warranties, liabilities, and remedies are determined by the applicable agreement and not by this public policy alone.

17. Updates to This Policy

Origin Data Lab may update this policy to reflect changes in website operations, field-collection workflows, technology, project requirements, service providers, business practices, or applicable legal obligations.

The current version and last-updated date will be displayed on this document and on the relevant website page. Where required or operationally appropriate, material changes may also be communicated through the website, application, email, operator channels, campaign instructions, or other designated methods.

Continued website use, field participation, or field-data delivery after an update does not override any separate agreement, consent requirement, or legal right that applies to the relevant person or engagement.

18. Contact

Questions concerning this Website & Field Operations Policy, website analytics, field participation, field data, privacy handling, access or deletion requests, safety, compensation, licensing, or governance may be submitted through the Origin Data Lab contact page.

Contact page: <https://origindatalab.io/contact.html>

General email: contact@origindatalab.io

Please include sufficient information to identify the relevant inquiry, account, collection mission, field-data delivery, project, or dataset where applicable.

Document control: Website and PDF versions should remain identical. The authoritative public version is the latest version published by Origin Data Lab.