EVERYDAY

API Customer Agreement

Package tracking services
Service levels, data handling and marketing disclosures

Contracting provider Jameson E Jones, doing business as Everyday Track, a sole proprietorship operating under the Everyday brand.

Version 1.0
Publication date: October 24, 2026
Effective for each customer upon affirmative electronic acceptance.

This agreement governs API customers. It includes the main terms and Schedules A-D. The required API acceptance checkbox does not itself authorize automated marketing calls, marketing texts, or unrestricted disclosure of personal information.

Contents

The section titles below link to their corresponding pages. All schedules form part of this agreement, subject to the scope and priority rules in Section 1.

1. Parties, scope and order of precedence 4

2. Defined terms and interpretation 4

3. Eligibility, authority and equal access 5

4. Electronic acceptance and account administration 5

5. Service description and shipment limitations 6

6. Upstream providers and limits on third-party rights 6

7. License, commercial integrations and permitted use 7

8. Acceptable use and prohibited conduct 8

9. Credentials and API security 8

10. Customer applications and End Users 9

11. Freemium access, Orders and plan limits 9

12. Payment, renewal, cancellation and refunds 10

13. Rate limits and technical operation 10

14. Availability and business API support 11

15. Updates, deprecation and service changes 11

16. Data handling and privacy responsibilities 12

17. Marketing communications and broker disclosures 12

18. Confidentiality 13

19. Intellectual property and feedback 13

20. Express commitments and warranty limitations 14

21. Limitation of liability 14

22. Third-party claims and indemnification 15

23. Investigation, suspension and restoration 15

24. Term, termination and post-cancellation records 16

25. Governing law and dispute resolution 16

26. General provisions and notices 17

Schedule A. Availability and business support 18

Schedule B. Data handling and processing terms 20

Schedule C. API marketing and broker-data notice 24

Schedule D. Requests, contacts and policy directory 28

1. Parties, scope and order of precedence

1.1 Provider. This API Customer Agreement, including Schedules A-D (the "Agreement"), is between Jameson E Jones, doing business as Everyday Track, a sole proprietorship operating under the Everyday brand ("Everyday," "we," "us" or "our"), and the individual or legal entity accepting it ("Customer" or "you"). Everyday's mailing address is 6339 Charlotte Pike, PMB 2015, Nashville, TN 37209, United States. Its website is https://everydaytrack.org and its contact email is support@everydaytrack.org.

1.2 API-specific scope. This Agreement governs access to Everyday's package-tracking application programming interface, associated credentials, API documentation and API support (together, the "API Service"). It does not replace the general website Terms of Service or Privacy Policy for activities outside the API Service. Using the consumer website, a public tracking link or a separately governed integration remains subject to the terms applicable to that activity.

1.3 Incorporated documents. A plan selection, checkout confirmation or mutually accepted written order that identifies the API Service is an "Order." An Order may specify purchased capacity, charges, billing periods and expressly agreed service commitments. Technical documentation governs implementation details, but cannot silently add fees, expand marketing permissions or remove an express contractual protection. Schedules A-D are incorporated into this Agreement.

1.4 Priority. Mandatory law prevails. A separately executed agreement prevails over this Agreement only where it expressly identifies the provision being varied. Schedule B controls processing of Customer Tracking Data; Schedule C controls the API-related marketing practices it describes; and Schedule A controls availability calculations and credits. Otherwise, this Agreement controls API-specific matters and an Order controls its stated commercial particulars. No document overrides a more protective, legally binding privacy promise concerning previously collected information without the notice and permission required to change that promise.

1.5 Effective date. This version is published October 24, 2026. It becomes effective for a Customer when that Customer affirmatively accepts it through the required signup checkbox or another electronic acceptance process expressly referencing this version. Publication alone does not bind a person who has not accepted the Agreement.

2. Defined terms and interpretation

2.1 API Client means an application, website, service, workflow or other integration operated by or for Customer that calls the API Service. **Authorized User** means a person Customer permits to administer its account or operate its API Client. **End User** means a person whose authorized shipment information is processed through an API Client, whether or not that person has an Everyday account.

2.2 Customer Tracking Data means tracking numbers submitted through the API and the associated shipment information processed or returned to fulfill Customer's requests. **Tracking Results** means the status information made available in a JSON response, including shipment events and other fields provided by the relevant source. A tracking number or Tracking Result can be personal information when it identifies or can reasonably be linked to a person or household.

2.3 Account Data means information used to establish, administer, bill, secure or support an API account, including contact details, account identifiers, credential records and relevant correspondence. **Operational Data** means request and service information necessary to authenticate, route, meter, secure and diagnose API activity. It is distinct from the tracking number submitted as the shipment input.

2.4 Marketing Contact Data means names, email addresses, telephone numbers and related source, permission and suppression records used for API advertising or marketing. It excludes Customer Tracking Data and API secret values. **Upstream Provider** means a carrier or tracking-data provider supplying shipment information or related infrastructure to Everyday, including Track123 and TrackingMore where used for an authorized request.

2.5 Applicable Law includes laws and binding requirements governing the relevant party, activity and individual. **Personal Information** includes personal data and equivalent terms under Applicable Law. "Including" introduces examples rather than an exhaustive list. "Written" includes an accessible electronic record. References to days mean calendar days unless expressly stated otherwise; business days exclude Saturdays, Sundays and United States federal holidays. A party's responsibility is limited to matters allocated to it by this Agreement and Applicable Law.

3. Eligibility, authority and equal access

3.1 Eligible customers. The API Service is available to individuals and organizations that can lawfully receive and use it. An individual accepting this Agreement must have legal capacity to enter into it. Where a parent or legal guardian may lawfully contract for a minor, that adult must accept and supervise the account. Children under 13 may not establish an API account or submit personal information directly to Everyday.

3.2 Organizational acceptance. If you accept for a company or another organization, you represent that you have authority to bind it. That organization is the Customer, and its Authorized Users must comply with the obligations applicable to their activities. An employee's acceptance does not authorize marketing to other employees or grant rights over their personal telephone numbers.

3.3 Nondiscrimination. Everyday does not deny access on the basis of race, color, religion, sex, gender, gender identity or expression, sexual orientation, national origin, ethnicity, disability, or another characteristic protected by Applicable Law. Objective restrictions based on legal capacity, sanctions, security, technical availability, lawful provider restrictions, payment or compliance with this Agreement are permitted when applied lawfully.

3.4 Geographic and legal limits. Customer must not use the API Service where receiving it is prohibited. Availability of the website does not establish that every API feature or marketing channel is available in every jurisdiction. Everyday may restrict a country, provider or feature where necessary to comply with law or an applicable upstream limitation. Mandatory consumer rights remain unaffected.

4. Electronic acceptance and account administration

4.1 Affirmative acceptance. Before API access is granted, Customer must select a required checkbox linking to this Agreement. Customer must have a reasonable opportunity to open, review and retain it. The party accepting agrees that its affirmative electronic action constitutes acceptance to the extent recognized by Applicable Law. No handwritten signature or blank signature page is required.

4.2 Acceptance evidence. Everyday may retain an account identifier, accepted version, acceptance event and associated technical evidence reasonably necessary to document the transaction. Such records are Account Data or Operational Data; they are not part of the shipment input. Customer may request a copy of the applicable agreement or available acceptance record by email with the subject "API Agreement Copy."

4.3 Accurate administration. Customer must maintain an email address it controls, keep billing and account information accurate, and ensure Authorized Users have the permissions appropriate to their duties. Customer must

promptly report loss of account control. It must not impersonate another person, misstate its authority or use another person's payment method without authorization.

4.4 Separate marketing choices. Acceptance of this Agreement is not, by itself, prior express written consent to automated marketing texts or artificial-voice or prerecorded marketing calls. It does not authorize Customer to consent on behalf of End Users, unrelated consumers or telephone subscribers. Optional channel-specific marketing consent must be obtained separately as described in Schedule C; refusal does not prevent access to an otherwise eligible free or paid API plan.

5. Service description and shipment limitations

5.1 Tracking workflow. The shipment input required for a standard API tracking request is a tracking number. Everyday processes the request, forwards the number to one or more appropriate Upstream Providers, and returns available tracking information to Customer's application in a JSON response. Authentication credentials and ordinary transport information are separate from that shipment input.

5.2 Response content. Depending on source availability, Tracking Results may include the identified carrier, current status, event descriptions, scan locations, timestamps, handoffs, delivery attempts and estimated or reported delivery information. Not every source supplies every field. An empty result, pending result or valid "not found" response does not necessarily mean that a shipment is invalid or that the API is unavailable.

5.3 Carrier detection. Where carrier detection is provided, it is an inference from available information. Number formats can overlap, tracking identifiers can be recycled, and shipments can pass between carriers. Customer must handle corrections, ambiguous results, duplicate events and changes in source data without representing detection as guaranteed.

5.4 Independent information service. Everyday is not a carrier, postal operator, shipper, retailer, insurer, freight forwarder or customs broker. It does not possess, transport, redirect, deliver or control packages. It does not determine a recipient's entitlement to goods or resolve loss, damage, theft, customs, refund or delivery disputes. Those matters must be directed to the responsible carrier, merchant or other relevant party.

5.5 Information limitations. Tracking Results can be delayed, incomplete, inaccurate, duplicated or out of sequence. Delivery estimates are estimates; a delivered status is a report from the source, not Everyday's independent verification. Customer must verify material shipment decisions with the responsible source and must not use the API as the sole evidence for a safety-critical or legally determinative decision.

6. Upstream providers and limits on third-party rights

6.1 Provider selection. Everyday may obtain tracking information from Track123, TrackingMore, carriers and other tracking-data providers. Provider references identify potential sources and do not represent exclusive relationships, endorsements, or a guarantee that any particular provider will serve a request. Everyday may change routing or sources to maintain lawful service and appropriate coverage.

6.2 Rights actually held. Everyday is responsible for securing the upstream rights needed to provide the API Service it offers. Customer's permissions under this Agreement extend only to rights Everyday owns or is authorized to grant. This Agreement does not amend an Upstream Provider's contract or create a sublicense, resale right or commercial-use right that the provider has not granted. Silence or ambiguity in a third-party policy is not treated as affirmative permission.

6.3 Communicated limitations. Everyday will communicate material source-specific restrictions that affect Customer's authorized use through the applicable Order, documentation or written notice. Customer must comply with restrictions actually applicable to the data or access it receives. A newly communicated restriction does not retroactively make previously authorized conduct a breach, but Customer must stop a use once notified that continuing it would infringe rights or violate law.

6.4 Loss of access or authorization. If an upstream right is withdrawn, restricted or unavailable, Everyday may substitute a lawful source, limit the affected data or suspend the affected functionality. If this materially removes a paid feature and Everyday cannot provide a substantially equivalent lawful alternative, Customer may terminate the affected paid service and receive a prorated refund of unused prepaid fees for that feature.

6.5 Independent conduct. Each provider remains responsible for its own systems and independent processing. Relevant provider policies may explain that processing. Referring Customer to those policies does not eliminate Everyday's responsibility for its own provider selection, disclosures, contractual commitments or legal obligations.

7. License, commercial integrations and permitted use

7.1 API access license. During the applicable subscription or free-access period, Everyday grants Customer a limited, nonexclusive right to access the API Service through the authorized interface and credentials, within the applicable limits, and to integrate it into lawful personal, internal-business and commercial applications. This license is subject to Sections 6 and 8 and ends when the applicable access is terminated.

7.2 Commercial flexibility. Customer may charge for its own application or service, display authorized Tracking Results to authorized End Users, and incorporate shipment-tracking functionality into customer-facing or white-label products. A commercial business model alone is not prohibited. Customer remains responsible for obtaining the rights and permissions needed for its own use and for preserving any applicable source-specific attribution.

7.3 Caching and records. Customer may retain or cache lawfully obtained Tracking Results to the extent necessary for an authorized tracking function, customer service, reconciliation or lawful recordkeeping, subject to privacy obligations and communicated provider restrictions. Cached results must not be represented as a newly refreshed carrier response. Customer must apply proportionate access controls and delete personal data when its retention is no longer justified.

7.4 Resale boundary. Customer may not transfer Everyday credentials, sublicense direct access to an upstream account, or supply a stand-alone replica or redistribution feed of third-party tracking data unless Everyday has confirmed that the applicable rights permit that arrangement. This condition is a rights limitation, not a blanket prohibition on competing applications or independently developed products.

7.5 Branding. Customer retains its own branding. No general Everyday attribution is required unless an accepted Order or an applicable source license requires it. Customer may truthfully identify Everyday as a technology provider, but use of Everyday's logo in a manner suggesting sponsorship, approval or partnership requires permission. No license to a carrier's trademark is granted by implication.

8. Acceptable use and prohibited conduct

8.1 Authorized shipments. Customer may submit only tracking numbers it is entitled to process, such as its own shipments or shipments processed with authority from a sender, recipient, merchant or other appropriate party. Possession of a tracking number does not, by itself, establish authority to exploit the associated information for unrelated purposes.

8.2 Privacy and physical safety. Customer must not use the API to stalk, harass, intimidate, unlawfully surveil or locate a person; infer private activity without a lawful basis; facilitate theft or redirection of goods; or discriminate unlawfully. It must not combine shipment data into unauthorized dossiers or use the API to make employment, credit, insurance, housing or other regulated eligibility decisions for which the data and service are not authorized.

8.3 Deception and infringement. Customer must not fabricate carrier scans, falsely represent a package as delivered, impersonate Everyday or a carrier, create deceptive delivery notices, conduct phishing, infringe intellectual property rights, or use Tracking Results to support fraudulent transactions. It must preserve material source qualifications and not deliberately mislead End Users about data freshness or accuracy.

8.4 Technical abuse. Customer must not bypass authentication or rate limits; rotate accounts or credentials to evade a limit; enumerate tracking numbers without authorization; introduce malware; impair availability; access nonpublic systems; harvest credentials; or perform intrusive security testing without written authorization. Good-faith reporting of a suspected vulnerability is permitted, but does not authorize exploitation or access to unrelated data.

8.5 Unlawful communications. Customer must not use shipment information to facilitate unlawful spam, unauthorized marketing calls or texts, or misleading advertising. A recipient's agreement to shipment updates is not automatically consent to promotional messaging. API access does not confer a right to use another person's contact details for marketing.

8.6 Proportionate enforcement. Everyday may investigate credible abuse, request a reasonable explanation and restrict the affected functionality. Measures will be proportionate to the risk where practicable. Restrictions necessary to address imminent harm, legal requirements or an active compromise may take effect immediately under Section 23.

9. Credentials and API security

9.1 Credential control. Customer must keep API keys confidential, restrict access to people and systems that need them, and use the available key-rotation options when a key is exposed or access responsibilities change. Customer must not send a complete active API key in ordinary support email. A redacted key identifier is normally sufficient to identify an issue.

9.2 Server-side storage. Customer must keep secret API keys on a controlled server in environment variables, a protected environment file or a suitable secret-management system. Environment files must not be committed to a public or shared source repository, served as public assets, embedded in browser JavaScript, included in a distributed mobile application, or exposed in logs. Naming a browser-build variable as an environment variable does not make its value secret.

9.3 Secure requests. Customer must use the designated encrypted API connection, validate certificates, protect its administration account, and limit credential permissions where the service offers that capability. Customer must avoid placing secrets or unnecessary personal information in URLs, client-visible error messages or diagnostic material.

9.4 Incident response. Upon discovering or reasonably suspecting a compromised key or unauthorized API activity, Customer must promptly revoke or rotate the affected key, contain its integration and notify

support@everydaytrack.org with the subject "API Security Incident." Everyday may revoke credentials or require reauthentication to contain a credible incident. Each party will reasonably cooperate on relevant investigation and remediation.

9.5 Allocation of responsibility. Customer is responsible for securing its API Client and its Authorized Users' access. Everyday is responsible for the security obligations allocated to it in Schedule B. Neither party guarantees absolute security. Customer is not responsible for activity to the extent it results from Everyday's breach rather than Customer's failure to fulfill its own obligations.

10. Customer applications and End Users

10.1 Customer's service. Customer independently determines the design, pricing, functionality and legal terms of its API Client. It must provide appropriate notices to its End Users explaining the tracking information it collects, why it is processed and that it is disclosed to Everyday and relevant tracking providers to fulfill tracking requests.

10.2 Lawful instructions. Customer must have a lawful basis and any necessary authority for Customer Tracking Data it submits. It must not provide unrelated names, email addresses, phone numbers, payment information, passwords, health information or government identifiers as additional shipment fields unless a separately authorized function specifically requires them. The standard tracking function requires the tracking number as its shipment input.

10.3 Responsible presentation. Customer must handle failures, delayed updates and absent fields reasonably; distinguish cached data from refreshed data; and avoid promises about delivery, coverage or accuracy exceeding those supported by the underlying information. Customer is responsible for its own notifications and for the permissions required to send them.

10.4 End-User rights. Customer must provide a reasonable channel for End Users to exercise applicable privacy rights concerning Customer's processing. Everyday will assist with requests concerning processing it performs on Customer's behalf as described in Schedule B. Neither party may require an End User to accept this commercial Agreement merely to submit a privacy request.

10.5 No transfer of marketing lists through the API. A tracking request does not subscribe an End User to marketing or instruct Everyday to create a marketing profile. Marketing Contact Data is governed separately by Schedule C. Customer may not treat this Agreement as permission to upload or disclose its own End Users' contact lists to a broker.

11. Freemium access, Orders and plan limits

11.1 Freemium model. Everyday offers API access through free and paid plans. The applicable plan determines available features, request allowances and other service limits. Free access is a limited service entitlement, not a promise of unlimited capacity or permanent availability of a particular free tier.

11.2 Disclosed commercial particulars. Before Customer incurs paid charges, Everyday must disclose the price, currency, billing period, included allowance, any usage-based or overage charge, and any recurring renewal arrangement in the plan selection or Order. Those accepted particulars form part of this Agreement. If a charge or overage rate has not been disclosed and accepted, this Agreement alone does not authorize it.

11.3 Free-to-paid transition. Creating a free account or exceeding a free allowance does not automatically authorize a paid upgrade. Everyday may stop or throttle further requests at the limit, offer an upgrade or apply an alternative the

Customer has expressly authorized. Everyday must obtain affirmative authorization before converting free access into a charged subscription.

11.4 Usage measurement. Metered units must follow the definition communicated for the selected plan. Customer may ask for a reasonable explanation of an apparent metering error. Everyday will investigate a good-faith billing dispute and correct verified errors. Customer must not deliberately manipulate request accounting or use multiple accounts to evade an allowance.

11.5 Capacity changes. Customer may request a different plan or additional capacity. Unless an accepted Order states otherwise, an upgrade and its price change begin only when Customer accepts them; a downgrade applies to the next billing period. A plan change does not expand rights to third-party data beyond Section 6.

12. Payment, renewal, cancellation and refunds

12.1 Payment authorization. Customer must pay properly disclosed and accepted charges when due. Where a payment service processes the transaction, Customer authorizes that service to process the agreed amount using the selected payment method. This Agreement does not represent that Everyday itself stores payment-card details. Customer is responsible for applicable transaction taxes other than taxes on Everyday's net income.

12.2 Recurring subscriptions. A subscription renews automatically only if the renewal arrangement, price or method of calculating it, billing interval and cancellation method were clearly disclosed and affirmatively accepted. Required renewal notices and consent requirements apply. Everyday may not treat silence about a previously undisclosed renewal arrangement as authorization to charge.

12.3 Cancellation. Customer may cancel through available account controls or by emailing support@everydaytrack.org with the subject "API Cancellation." Customer should identify the account and request that further renewals stop; no special explanation is required. Unless Customer asks for immediate closure or Applicable Law requires otherwise, paid access continues through the current paid period and cancellation prevents subsequent renewal. Reasonable account verification may be requested.

12.4 Refunds. Except as required by law or expressly provided in this Agreement or an Order, fees for service already supplied and consumed usage are nonrefundable. A refund of unused prepaid fees applies where Everyday ends a paid service for its convenience before the prepaid period ends or materially fails to supply it under Sections 6, 15 or 24. Availability credits are addressed in Schedule A. Duplicate or incorrectly assessed charges will be corrected.

12.5 Price changes and overdue accounts. Everyday will provide at least 30 days' notice of a recurring price increase, and an increase will not apply before the next renewal following that notice. Customer may cancel before it takes effect. Everyday may suspend materially overdue paid access after reasonable notice and an opportunity to resolve the issue. Good-faith disputes over a charge will be considered before disproportionate collection or suspension measures are taken.

13. Rate limits and technical operation

13.1 Applicable limits. Customer must observe the rate, concurrency, volume and resource limits disclosed for its plan through the Order, account controls, API documentation or response headers. Everyday may apply additional reasonable protections during an active security or availability incident. A temporary protective limit does not authorize an undisclosed fee.

13.2 Request behavior. Customer must implement reasonable retry intervals and backoff, respect communicated retry instructions, avoid duplicate calls where practicable, and prevent uncontrolled retry loops. A rate-limited or invalid request is not a service outage merely because it fails to produce shipment data.

13.3 Changes to limits. Everyday will give reasonable advance notice of a material reduction in paid capacity, ordinarily at least 30 days, unless a legal requirement, upstream restriction or urgent security event requires faster action. Customer may use the termination and unused-fee remedies in Section 15 if a material reduction substantially impairs a purchased feature.

13.4 Technical independence. Customer remains responsible for its own internet access, application hosting, data storage and integration code. Everyday does not warrant compatibility with an undocumented interface or a modified third-party client. Customer must not depend on undocumented behavior that could reasonably change without altering the documented function.

14. Availability and business API support

14.1 Service commitment. Everyday commits to 99% Monthly Availability for the API Service, measured and qualified as described in Schedule A. This is a contractual service-level commitment, not a representation about independently audited historical uptime and not a guarantee that a carrier will publish a particular scan or deliver a package.

14.2 Support channel and hours. Email is the support channel for business API customers. The business API support window is 6:30 a.m. to 9:30 p.m. Central Time, using America/Chicago and its daylight-saving changes. Messages may be sent at any time. The support window is not a guaranteed response or resolution time and does not provide a telephone or emergency-response service.

14.3 Scope of support. Support covers account access, API keys, documented API behavior, billing, service incidents and reasonable integration questions. It does not include operating Customer's application, developing custom code, carrier claims, delivery intervention or guaranteed support for unrelated third-party systems unless an Order expressly provides otherwise.

14.4 Business-specific policy. These support hours apply to business customers using the API Service. They do not establish support hours for the general consumer website or a separate product. This Agreement is publicly accessible when posted; inclusion of the hours here does not make them confidential.

15. Updates, deprecation and service changes

15.1 Continuing improvement. Everyday may maintain and update the API, change providers, add optional features and modify technical implementation. It will use reasonable care to preserve documented functionality during an existing paid term. Additive fields and corrections that do not materially impair the documented function may be introduced without a new agreement.

15.2 Material adverse changes. Everyday will ordinarily provide at least 30 days' notice before a breaking change, retirement of a paid endpoint or material reduction in purchased functionality. The notice will identify the affected function and any practical migration option. A shorter period may be used where necessary for law, security, upstream rights or circumstances that cannot reasonably be postponed.

15.3 Customer choices. If a material adverse change substantially impairs a paid feature and a substantially equivalent alternative is not available, Customer may cancel that affected service and receive a prorated refund of

unused prepaid fees. Customer must reasonably cooperate with lawful migration steps; it is not required to accept an additional paid product as the only way to preserve the value of an existing commitment.

15.4 Changes to this Agreement. Everyday may publish a revised agreement with a new version and effective date. Material changes will be communicated to affected customers before taking effect, ordinarily at least 30 days in advance unless a shorter period is legally necessary. Everyday will obtain renewed acceptance where required. Changes operate prospectively and do not retroactively alter a pending dispute or authorize a new use of previously collected personal information without required notice and permission.

16. Data handling and privacy responsibilities

16.1 Shipment input and other records. A standard tracking call requires the tracking number as its shipment input. Authentication, account administration, transport routing, usage measurement, security and support separately involve the account and operational information described in Schedule B. The limited shipment input does not imply that those separate functions operate without other information.

16.2 Restricted tracking purposes. Everyday processes Customer Tracking Data to fulfill authorized tracking requests and necessary related security, support and legal functions. It does not add tracking numbers, shipment histories or API keys to broker marketing lists, use them to construct advertising profiles, or combine them with broker contact data for targeted advertising.

16.3 Separate contact records. Everyday's processing of Marketing Contact Data, including contacts obtained from brokers or added to broker-hosted lists, is described in Schedule C. Such processing must not be disguised as necessary delivery of a tracking result. API account closure, marketing suppression, disclosure opt-out and data deletion are distinct actions with distinct effects.

16.4 Rights and retained obligations. A person may use the request form or email channels in Schedule D. Everyday remains responsible for duties imposed on it by Applicable Law, including legally required notices, access, correction, deletion, objection, opt-out, security, consent and breach response. Neither contractual acceptance nor a reference to another company's privacy policy waives those duties.

17. Marketing communications and broker disclosures

17.1 Express disclosure. Everyday obtains names, email addresses and telephone numbers from data brokers, including Salesgenie and ZoomInfo, for advertising and marketing. Everyday also maintains marketing lists in Salesgenie and may add contact information provided directly to Everyday, subject to the boundaries, notices, permissions and choices in Schedule C.

17.2 Independent marketing use. Where properly disclosed and lawfully permitted, adding contact information to a broker's system may disclose it to that broker directly or indirectly, and the broker may use permitted information for its own or others' advertising and marketing. The legal treatment depends on the actual arrangement, including whether it constitutes a sale, sharing or targeted-advertising disclosure. Calling a transfer indirect does not remove applicable obligations.

17.3 Communications. Everyday may market by email and, where the required permission exists, by automated text and artificial-voice or prerecorded call. A purchased list, a broker's assertion of permission, an account registration or the required API checkbox is not alone sufficient evidence of every permission required for those channels. Everyday must verify an adequate basis before initiating the relevant campaign.

17.4 Protected choices. Marketing consent is optional and can be withdrawn. Where Applicable Law requires an opt-out or consent for broker disclosure, Everyday must provide and honor it. Refusing marketing does not cancel a paid plan, and cancelling a plan does not automatically communicate every privacy preference. Schedule C governs these distinctions without restricting any statutory right.

18. Confidentiality

18.1 Covered information. Confidential Information means nonpublic information one party discloses to the other that is identified as confidential or reasonably should be understood to be confidential, including nonpublic technical documentation, security information, credentials, business information and Customer Tracking Data. Information does not lose protection merely because it is transmitted electronically.

18.2 Permitted handling. The receiving party may use Confidential Information only to perform or exercise rights under this Agreement, and may disclose it to personnel and permitted providers that need it for that purpose and are subject to appropriate confidentiality obligations. It must use reasonable care to protect the information, at least the care it uses for its own similarly sensitive information.

18.3 Exceptions. Confidentiality does not apply to information the recipient can demonstrate became public without its breach, was already lawfully known without restriction, was independently developed without use of protected information, or was lawfully obtained from another source without a duty of confidence. Personal Information remains subject to applicable privacy requirements even if a confidentiality exception applies.

18.4 Required disclosures. A party may disclose information to comply with law or binding legal process, limiting disclosure where reasonably possible and providing advance notice when lawful and practicable. Nothing prevents reporting suspected unlawful conduct to a regulator, seeking legal advice, or exercising a protected whistleblower right.

18.5 Duration and marketing carve-out. Confidentiality continues for three years after the relevant disclosure, and for trade secrets while they remain trade secrets under Applicable Law. Credentials and Personal Information remain protected for as long as protection is required by their nature or Applicable Law. The specific, lawful contact disclosures described in Schedule C do not authorize disclosure of unrelated confidential business information or Customer Tracking Data.

19. Intellectual property and feedback

19.1 Reserved ownership. Everyday and its licensors retain their rights in the API Service, its software, documentation, interface, branding and original materials. Customer retains its rights in its API Client and submitted materials. Carriers and Upstream Providers retain their rights in their respective systems, marks and data. No party acquires another party's rights except the express permissions in this Agreement.

19.2 Processing permission. Customer authorizes Everyday to transmit, process and return Customer Tracking Data only as necessary to provide the API Service and fulfill the limited related purposes in Schedule B. This permission does not transfer ownership, authorize unrelated advertising use, or eliminate obligations to End Users.

19.3 Feedback. Customer may voluntarily provide ideas or suggestions. Everyday may use that feedback to improve its services without payment or an obligation to implement it. This permission does not cover Customer's confidential information, Personal Information, source code or other materials merely because they appear in a support request.

19.4 No implied endorsement. Neither party may issue a case study, endorsement or press release naming the other as a partner without permission. Truthful identification necessary to describe an integration or make a legal disclosure is permitted. Neither party may remove another's required ownership notices or use marks in a confusing or deceptive way.

20. Express commitments and warranty limitations

20.1 Express performance commitments. Everyday will use reasonable care and skill to provide the API Service and perform its express obligations, including the service-level and data-handling commitments in this Agreement. Customer represents that it has authority to accept the Agreement and to submit the tracking numbers and instructions it provides.

20.2 Qualified service disclaimer. Except for express commitments in this Agreement or an accepted Order, and to the extent permitted by Applicable Law, the API Service and third-party Tracking Results are provided "as is" and "as available." Everyday disclaims implied warranties of merchantability, fitness for a particular purpose and noninfringement only to the extent such disclaimers are lawful. This clause does not disclaim Everyday's responsibility to obtain the rights required by Section 6 or perform its express privacy and security obligations.

20.3 No shipment warranty. Everyday does not warrant the accuracy, completeness or timeliness of third-party scans; universal carrier coverage; a particular delivery date; successful customs clearance; or the condition, existence or location of goods. It does not warrant that the API will be uninterrupted or error-free at every moment. Schedule A governs the specific availability commitment.

20.4 Mandatory rights preserved. Nothing excludes a warranty, remedy, duty or consumer protection that Applicable Law does not permit the parties to exclude. A person acting as a consumer retains the protections applicable to that status regardless of how a plan is labeled. Statements from an unauthorized third party do not amend this Agreement.

21. Limitation of liability

21.1 Excluded loss categories. To the extent permitted by Applicable Law, neither party is liable to the other for indirect, incidental, special, exemplary, punitive or consequential damages, or for lost profits, revenue, goodwill or business opportunity arising from this Agreement. This exclusion applies regardless of legal theory and even if the possibility of such loss was identified, subject to the exceptions below.

21.2 General cap. Subject to Section 21.3, each party's aggregate liability arising from this Agreement will not exceed the greater of USD 100 or the total API Service fees paid or payable by Customer for the 12 months immediately preceding the event giving rise to the claim. Related claims arising from substantially the same event are treated as one event. The cap does not reduce Customer's obligation to pay properly incurred fees or Everyday's obligation to provide an expressly owed refund or service credit.

21.3 Exceptions. The exclusions and cap do not limit liability for fraud, willful misconduct, gross negligence where limitation is prohibited, death or personal injury where limitation is prohibited, infringement or misappropriation of the other party's intellectual property, or any liability or individual privacy remedy that cannot lawfully be limited. They do not excuse performance of privacy requests, confidentiality duties, breach notifications or other continuing obligations. Indemnity obligations remain subject to the cap except to the extent a listed exception applies.

21.4 Shipment and third-party matters. Everyday is not responsible as a carrier or insurer for loss, theft, damage, misdelivery or delay of a shipment. This allocation does not exclude a claim based on Everyday's own breach where Applicable Law permits that claim. A provider's independent failure is not automatically Customer's responsibility.

21.5 Proportionate application. These provisions allocate foreseeable commercial risk while preserving nonwaivable rights. If a limitation is unenforceable for a particular claim, it applies only to the maximum lawful extent and does not invalidate unrelated provisions. No clause imposes a shortened statutory filing deadline on a consumer.

22. Third-party claims and indemnification

22.1 Customer responsibility. For business use, Customer will defend Everyday against a third-party claim to the extent caused by Customer's knowing submission of unauthorized tracking numbers, unlawful use of Tracking Results, infringement by its own application or materials, or material breach of the acceptable-use obligations, and will pay covered damages and reasonable defense costs finally awarded or agreed in an authorized settlement.

22.2 Limits on indemnity. Customer does not indemnify Everyday for Everyday's own unlawful marketing, insufficient upstream licensing, breach of this Agreement, negligence or willful misconduct, or for a third-party claim caused by Everyday's alteration or use of data outside Customer's lawful instructions. This indemnity does not apply to personal consumer use where prohibited or unfair under Applicable Law and remains subject to Section 21.

22.3 Claim procedure. Everyday must promptly notify Customer of a covered claim, provide reasonable cooperation at Customer's expense, and allow Customer to control the defense using competent counsel. Delay in notice reduces responsibility only to the extent it materially prejudices the defense. Everyday may participate through its own counsel at its own expense.

22.4 Settlement protection. Customer may not settle a claim in a way that admits fault by Everyday, imposes nonmonetary obligations on it, or fails to release it from the covered claim without Everyday's written consent, which will not be unreasonably withheld. Everyday may take reasonable protective action where necessary to prevent imminent harm or a conflict of interest, with costs allocated according to the parties' actual responsibility.

23. Investigation, suspension and restoration

23.1 Grounds. Everyday may suspend or restrict affected API access where reasonably necessary to address suspected credential compromise, material abuse, an unlawful request, an applicable upstream restriction, a material contractual breach or an unpaid undisputed amount following notice. Suspension must not be imposed merely because a person exercises privacy rights or declines optional marketing.

23.2 Notice and opportunity to cure. Where practicable and lawful, Everyday will explain the basis for a suspension and provide a reasonable opportunity to remedy the issue. Immediate action may be taken for an active attack, imminent harm, a legal requirement or a comparable urgent circumstance. Everyday may withhold details that would expose another person's data, compromise security or violate law.

23.3 Scope and review. Everyday will consider whether restricting an affected key, endpoint or account function can reasonably address the risk. Customer may request review by emailing support@everydaytrack.org with the subject "API Suspension Review." Everyday will consider relevant evidence and restore access when the reason for suspension has been resolved and restoration is lawful.

23.4 Charges during suspension. Valid charges already incurred remain payable. If suspension results from Everyday's error or a convenience decision rather than Customer's breach, Everyday will reasonably adjust affected paid charges or apply the applicable refund or availability remedy. Customer must not create replacement accounts to evade a valid suspension.

24. Term, termination and post-cancellation records

24.1 Term and termination by Customer. This Agreement continues while Customer has API access or an active paid commitment. Customer may stop using free access or cancel paid access under Section 12. A request for immediate account closure terminates the access affected by that request, subject to verification and settlement of properly incurred charges.

24.2 Termination by Everyday. Everyday may terminate for a material breach not cured within 15 days after written notice, or immediately where the breach is incapable of cure, continued service would be unlawful, or urgent security or safety circumstances require termination. Everyday may discontinue a free plan with reasonable notice or end a paid service for convenience on at least 30 days' notice, refunding unused prepaid fees for service it does not supply.

24.3 Consequences. On termination, the affected API license ends and Customer must stop calling the service with terminated credentials. Everyday may revoke those credentials. Customer may retain previously received records only where its rights, privacy duties and any applicable source restrictions permit retention; termination does not create a new right to redistribute them.

24.4 Cancellation is not automatic erasure. Cancelling API access does not automatically erase every account, business, marketing or suppression record. Retained information remains governed by Schedules B and C. Customer may separately request deletion, marketing suppression or an opt-out of broker disclosure through Schedule D. A valid request may also be made by another method required by law. The absence of a deletion request does not authorize retention beyond a lawful and necessary purpose.

24.5 Survival. Payment obligations already incurred, ownership provisions, lawful confidentiality duties, data-handling obligations for retained information, applicable disclaimers and liability limits, claim procedures and dispute provisions survive to the extent necessary to give them effect. Marketing permission does not become irrevocable because the commercial relationship has ended.

25. Governing law and dispute resolution

25.1 Governing law. Tennessee law and applicable United States federal law govern this Agreement, without applying conflict-of-law rules that would displace that choice. This choice does not deprive a consumer or data subject of mandatory protections of a jurisdiction whose law applies notwithstanding the choice.

25.2 Informal resolution. Before bringing a claim, the parties will attempt in good faith to resolve it through written notice describing the issue and requested resolution. Customer may send notice to support@everydaytrack.org with the subject "API Legal Dispute" or to Everyday's mailing address in Schedule D. Everyday will use Customer's current account contact information. The parties will ordinarily allow 30 days to discuss a resolution.

25.3 Courts. Subject to mandatory consumer venue rules, a dispute that cannot be resolved informally may be brought in the state courts located in Davidson County, Tennessee, or, where federal jurisdiction exists, the United States District Court for the Middle District of Tennessee. Each party consents to those courts for disputes properly brought there. A consumer may use any court or small-claims forum that mandatory law makes available.

25.4 No mandatory arbitration. This Agreement does not require arbitration or waive the right to a jury trial or participation in a class proceeding where available under Applicable Law. It does not restrict complaints to regulators, privacy authorities or law-enforcement agencies.

25.5 Urgent relief and deadlines. The informal process does not prevent a party from seeking urgent injunctive relief, protecting evidence, filing before an applicable limitation period expires, or exercising a nonwaivable statutory remedy. Neither party must disclose unnecessary personal information or privileged legal advice as a condition of seeking a remedy.

26. General provisions and notices

26.1 Entire API agreement. This Agreement and accepted Orders state the parties' agreement about the API Service, subject to separate agreements expressly identified in Section 1. They do not extinguish independent privacy rights or an applicable earlier promise about Personal Information. A Customer purchase-order form does not add conflicting legal terms unless Everyday expressly accepts them in writing.

26.2 Assignment. Customer may not transfer its account or contractual rights to another person without Everyday's reasonable approval, except as permitted in an accepted Order. Everyday may assign this Agreement in a bona fide reorganization or transfer of the relevant business, provided the successor assumes applicable obligations and Personal Information remains subject to required safeguards. Assignment is not permission to disregard a privacy notice or consent limitation.

26.3 Events beyond reasonable control. A party is not liable for delay to the extent caused by circumstances beyond its reasonable control that it could not reasonably prevent or mitigate, provided it takes reasonable steps to limit the effect and resumes performance when practicable. This provision does not excuse payment for service already supplied, required privacy protection, or refunds for service permanently not provided. Schedule A governs the treatment of excluded availability events.

26.4 Severability and waiver. If a provision is unenforceable, it will be limited to the extent necessary and the rest of the Agreement remains effective where the essential bargain can continue. Failure to enforce a provision once is not a continuing waiver. A waiver must be clear and authorized.

26.5 Relationship. The parties are independent contractors. This Agreement does not create a partnership, agency, employment relationship, carrier relationship or joint venture. It does not authorize either party to bind the other. No third-party beneficiary is created, except that this clause does not remove rights a person has independently under Applicable Law.

26.6 Notices and contact subjects. Routine notices may be delivered through Customer's account or current email address. Material contractual notices must be reasonably calculated to reach Customer. The recommended email subjects in Schedule D help route requests but are not mandatory words for an otherwise clear legal or privacy request. Email notices do not replace formal service of legal process where law requires another method.

Schedule A. Availability and business support

A.1 Scope of the 99% commitment

Everyday commits to 99% Monthly Availability of the authorized API request-processing function. The commitment applies to active free and paid accounts, subject to the exclusions below; monetary service credits apply only where the affected service has a recurring fee. A separately accepted Order may expressly provide a different service level.

The measured function is Everyday's ability to accept valid, authenticated requests within Customer's applicable limits and return a technically valid API response. A deliberately returned error caused by Everyday's own failure to provide the documented function is not counted as successful operation merely because it is formatted as JSON. A genuine, correctly handled "not found," pending or no-new-events result is a valid response.

The commitment does not guarantee the publication of new scans, the accuracy of a carrier's record, the correctness of an estimated delivery date, or availability of every source or carrier. An application can be available while a particular carrier has not provided new information.

A.2 Calculation and measurement

"Monthly Availability" is 100 multiplied by the difference between Eligible Minutes and Unavailable Minutes, divided by Eligible Minutes. Eligible Minutes are the minutes in the calendar month during which the affected API access was active, less minutes excluded under A.3. Unavailable Minutes are Eligible Minutes during which Everyday's controlled systems could not perform the documented request-processing function for Customer's valid requests.

The calendar month and service records use Central Time, America/Chicago. For an account active for only part of a month, only the active portion is measured. If there are no Eligible Minutes, no availability percentage or availability credit is calculated for that period.

Everyday's service records and reasonably reliable Customer evidence are used together to investigate an outage. Customer may provide timestamps, endpoint identifiers, response codes and redacted request references. A lack of a public status-page entry is not conclusive proof that no outage occurred. Neither party is required to expose an active secret key or unrelated personal data to support a claim.

A.3 Exclusions and maintenance

Excluded events are failures caused by Customer's application or infrastructure; invalid credentials or malformed requests; traffic exceeding an applicable communicated limit; a lawful suspension attributable to Customer's breach; general internet failures outside Everyday's control; and an Upstream Provider's independent outage or withdrawal of a required right that Everyday could not reasonably prevent or mitigate. An event is excluded only to the extent it actually caused the unavailability.

An upstream-related failure caused by Everyday's own integration defect, avoidable misconfiguration or failure to maintain its required account is not automatically excluded. Ordinary maintenance of Everyday-controlled systems counts as unavailability when it interrupts the measured function. Everyday will give advance notice of planned material interruptions where reasonably practicable and use reasonable efforts to minimize disruption.

Availability exclusions do not excuse Everyday's separate duties to communicate material service changes, address security incidents, protect retained information or refund unused prepaid fees where this Agreement requires a refund.

A.4 Availability credits

If Monthly Availability falls below 99%, a paid Customer may request a service credit equal to 10% of the recurring subscription fee attributable to the affected API Service for that month. For a prepaid annual subscription, the monthly fee is one-twelfth of the annual recurring fee. Taxes, one-time charges and unrelated products are excluded from the calculation. A free plan has no monetary credit.

Customer must submit an ordinary availability-credit request within 30 days after the affected month ends to support@everydaytrack.org, with the subject "API Availability Credit," identifying the account, affected period and reasonable supporting details. Everyday will review the evidence in good faith. The request window does not shorten a statutory claim period or prevent a remedy that cannot lawfully be restricted.

Approved credits are applied to the next invoice for the affected service. If the paid service ends before the credit can reasonably be used, Everyday will refund the unused approved credit. The maximum standard availability credit for a month is 10% of that month's recurring fee; multiple incidents do not multiply that amount.

These credits are the contractual remedy for failure to meet the availability percentage alone. They do not eliminate an expressly owed unused-fee refund, a remedy for a different breach such as unlawful disclosure of Personal Information, or a right that Applicable Law does not permit the parties to limit.

A.5 Support hours and case handling

Business API email support is available during the daily window of 6:30 a.m. to 9:30 p.m. Central Time, America/Chicago. Daylight-saving changes follow that time zone. Emails sent outside the window remain valid submissions and may be handled in a later support window. These hours do not set permissible hours for telemarketing calls or texts, which depend on the recipient's location and Applicable Law.

Use "API Support" for integration questions, "API Billing" for charges, and "API Security Incident" for a suspected compromise. Include a concise description, account contact and redacted diagnostics. Support prioritization may reflect severity, scope and security risk. There is no guaranteed first-response or resolution deadline unless an accepted Order expressly establishes one.

Customer must not rely on support email for an emergency involving personal safety, urgent carrier intervention or time-critical preservation of legal rights. Security and privacy obligations continue outside support hours to the extent required by Applicable Law.

Schedule B. Data handling and processing terms

B.1 Distinct categories and purposes

Shipment input. The standard tracking request requires a tracking number, which Everyday transmits to an appropriate Upstream Provider to retrieve available shipment information. Customer should not submit unrelated personal fields. Returned JSON can contain shipment information supplied by the provider even though Customer's request input consisted only of a tracking number.

Account and support information. Contact details and account records are processed to establish access, administer the customer relationship, handle correspondence, manage paid entitlements where applicable, and record legal notices and acceptance. A support message can contain information that would not otherwise appear in an API request. Customer should redact unnecessary personal or confidential information.

Authentication and operational information. API credentials or credential identifiers, request routing information and relevant technical metadata are processed as needed for authentication, delivery, usage limits, security and diagnosis. A network request exposes transport information such as an originating IP address to relevant infrastructure. This Agreement does not promise that all hosting, security and provider systems operate without logs.

Marketing information. Names, email addresses, phone numbers and associated preference records used for advertising are governed by Schedule C. Salesgenie lists hold marketing contacts; they are not an authorized repository for Customer Tracking Data under this Agreement. The existence of a marketing list does not determine where every operational or upstream record is stored.

B.2 Roles and permitted instructions

Each party is responsible for the processing purposes it independently determines. Everyday acts independently in administering its API business relationship, securing its service, satisfying legal duties and conducting its own permitted marketing. Customer independently determines its application, End-User relationship and lawful purposes for submitting shipment requests.

To the extent Everyday processes Customer Tracking Data solely on Customer's behalf and Applicable Law treats Everyday as a processor or service provider, B.3-B.8 are the parties' processing terms. An actual carrier or tracking provider may have a different role for its own shipment records; describing a party as a processor does not override its factual or legal role.

Customer's documented instructions are to receive authorized tracking numbers, route them to appropriate authorized tracking providers, receive and normalize available results, return them to the API Client, and perform necessary security, support and lawful retention functions described in this Agreement. Customer may give additional lawful written instructions consistent with the service. Everyday must inform Customer if it reasonably believes an instruction violates applicable data-protection law and may suspend that instruction while the issue is resolved.

B.3 Processing description and restrictions

The subject matter is on-demand package-tracking information. Processing lasts for the period of API use and any limited post-termination period required for lawful retention and deletion. Its nature includes transmission, retrieval, organization, response delivery, incident investigation and deletion. The relevant people may include senders, recipients, Customer's staff and authorized End Users. The data consists of tracking numbers, associated shipment information and necessary related operational records.

Everyday must not use Customer Tracking Data for unrelated advertising, sell it as a contact dataset, add it to Salesgenie or ZoomInfo marketing lists, or combine it with broker data to create advertising profiles. Where processor or service-provider restrictions apply, Everyday must not retain, use or disclose that data outside the permitted service and legal purposes, or outside the direct business relationship, except as Applicable Law permits.

Everyday must ensure that persons authorized to handle Customer Tracking Data are subject to confidentiality duties and access only information reasonably needed for their work. Customer may take reasonable steps to verify compliance with these processing restrictions and request remediation of an identified unauthorized use. Everyday must notify Customer if it can no longer meet an applicable processing obligation.

B.4 Security obligations

Everyday must maintain technical and organizational safeguards proportionate to the nature of the data and the service, including encrypted transport for the API, controls over administrative and credential access, reasonable separation of customer access, key revocation or rotation capability, and incident-response procedures. These are contractual safeguards; this Agreement does not assert a particular independent security certification or audit that has not been provided.

Customer must secure its API Client, devices, account and keys as required by Section 9. It must restrict tracking information to authorized people, avoid unnecessary public tracking links and prevent disclosure of secrets in client-side builds. Each party must minimize personal information in troubleshooting records and support attachments.

Neither party may intentionally send unnecessary sensitive information through the standard tracking field. A tracking event may nevertheless reveal a facility or approximate location; it must not be treated as anonymous merely because a name is absent. The parties must account for the risk of linking a tracking number to a person, household or purchase.

B.5 Providers, subprocessors and transfers

Customer authorizes use of necessary tracking providers, including Track123 and TrackingMore where Everyday holds the required rights, and necessary infrastructure providers operating under appropriate agreements. A marketing broker is not thereby authorized to receive Customer Tracking Data. Everyday must impose appropriate contractual protections on a provider acting as its subprocessor and remains responsible for its subprocessor obligations to the extent required by Applicable Law.

Everyday will make current information about material subprocessors and relevant processing locations available on request. Where a new subprocessor requires notice and an opportunity to object under Applicable Law, Everyday will provide that opportunity before the new processing begins, ordinarily with 15 days' notice unless an urgent lawful replacement is necessary. Customer may raise reasonable data-protection objections. If no reasonable solution is available, either party may end the affected processing, with a refund of unused prepaid fees for service Everyday cannot provide.

Data may be processed in the United States and countries where authorized providers operate. Where a transfer is legally restricted, the parties must establish the required transfer mechanism and safeguards before that transfer. This Agreement alone is not a representation that standard contractual clauses, a certification or another transfer mechanism has been executed or applies. Everyday may restrict an affected transfer until an appropriate mechanism is in place.

B.6 Incidents and assistance

If Everyday becomes aware of a personal-data breach affecting Customer Tracking Data processed on Customer's behalf, it must notify Customer without undue delay and within any shorter period required by Applicable Law. Information provided as reasonably available will include the nature of the incident, affected data categories, known or likely consequences, measures taken or proposed, and a contact for follow-up. An initial notice may be supplemented as investigation continues.

Each party will reasonably cooperate to contain the incident, preserve relevant evidence and support legally required notifications. Notification is not an admission of liability. Customer remains responsible for notifications concerning its independent processing, while Everyday remains responsible for notifications and duties imposed on it directly.

Taking account of the service and available information, Everyday will reasonably assist Customer with data-subject requests, appropriate security assessments, impact assessments and regulator consultations required for processing under this Schedule. It may verify Customer's authority and avoid disclosing another customer's information. A request from an End User concerning Customer's own processing may be referred to Customer unless law requires Everyday to act directly.

B.7 Retention, deletion and return

Everyday retains information only while reasonably necessary for the stated purpose and legitimate legal, accounting, security, dispute or suppression requirements. Relevant criteria include account activity, the need to complete a request, the category's sensitivity, applicable limitation and recordkeeping periods, and the feasibility of deleting residual backup copies. Storage availability alone is not a reason for indefinite retention.

Cancellation ends or changes API access; it does not necessarily delete Account Data or independently controlled marketing records. Customer may request deletion or a copy of its own retained information through Schedule D. Everyday will explain any material legal exception requiring retention and limit use of retained records to the exception. A general policy of retaining all records until a form is submitted cannot override a statutory deletion or storage-limitation duty.

For Customer Tracking Data processed solely on Customer's behalf, Everyday will, on termination and at Customer's lawful choice, return available retained data or delete it, unless law requires retention. Everyday is not required to recreate data it never retained or retrieve records that a carrier independently controls. Copies held solely in backups will be isolated from ordinary use and removed through the applicable deletion cycle, subject to law; they must not be restored for marketing.

Minimal suppression records may be retained to prevent a deleted contact from being imported into marketing again. Such records must not be reused as campaign audiences. Deleting customer data, stopping marketing and preserving proof of compliance may therefore involve different records and different lawful retention periods.

B.8 Accountability and reasonable verification

Where processor law applies, Everyday will make available information reasonably necessary to demonstrate compliance and permit a proportionate review by Customer or an independent auditor bound by confidentiality. Reviews should ordinarily begin with documents and existing assurance materials, be arranged on reasonable notice, minimize disruption and protect other customers' data and security. An urgent regulator request or credible material incident may require a different procedure.

Neither party must disclose privileged legal advice, active secrets or another person's unrelated Personal Information. Routine extraordinary assistance or an on-site review may be subject to reasonable, disclosed costs agreed in advance, but Everyday will not charge a fee that unlawfully obstructs an individual's rights or shift the cost of remedying its own material breach to Customer.

If a further written arrangement is mandatory for a particular regulated use or transfer, the parties must put it in place before that activity. A Customer must not assume that acceptance of a general API agreement authorizes processing health records, regulated financial records or other sensitive datasets not needed for ordinary shipment tracking.

Schedule C. API marketing and broker-data notice

Marketing disclosure. We contact data brokers to obtain your information for advertising and marketing. The contact information involved is names, email addresses and phone numbers. We use sources including Salesgenie and ZoomInfo, maintain contact lists in Salesgenie, and may disclose eligible contact information to brokers for independent advertising uses, subject to the limits and choices below. Tracking numbers, shipment histories and API keys are excluded from these marketing lists.

C.1 Scope and responsible business

Jameson E Jones, doing business as Everyday Track, is responsible for Everyday's collection, use and disclosure described in this Schedule. It covers API account contacts and people contacted to market the API, including prospects who have not purchased or accepted the Agreement. A prospect is not bound to commercial terms merely because Everyday holds their contact information; the privacy information and choices in this Schedule are available without contractual acceptance.

This Schedule supplements API-related disclosures. It does not amend the general website Privacy Policy for ordinary website users or override a prior promise that their data will not be sold or disclosed for independent advertising. Contact information from a consumer-platform account may enter the activities described here only after the person receives the applicable notice and Everyday obtains any permission required to make that change. API Customer acceptance cannot supply consent for other consumers or Customer's End Users.

C.2 Sources and categories

Everyday obtains Marketing Contact Data from brokers and marketing partners, including Salesgenie and ZoomInfo, and may obtain it directly from an individual through an account, inquiry or permitted signup. The relevant contact fields are names, email addresses and telephone numbers. Not every source or contact has every field.

Everyday also processes information needed to establish the source and permitted use of a contact, record a marketing choice, document applicable consent and prevent further contact after an objection. A record's presence on a broker list does not establish that the person is an existing Everyday customer, that the information is correct, or that permission exists for every communication channel.

Everyday does not use Customer Tracking Data, saved shipment history or website browsing behavior to enrich these contact records or construct shipment-based advertising profiles under this Agreement. It does not use these contact lists to make automated decisions producing legal or similarly significant effects about a person.

C.3 Purposes and list storage

Everyday uses eligible contact records to advertise and market its API, communicate relevant offers, manage campaigns, maintain the accuracy of its lists and administer consent, objections and suppression. Marketing lists are stored in Salesgenie. Adding a contact to a list is distinct from sending a campaign and must respect restrictions applicable to both actions.

Directly provided contact details may be added to a list only for uses consistent with the notice and permissions applicable when the information is obtained, or with a lawfully implemented change. Providing an email address for account security or a phone number for a support issue is not automatically permission for every independent broker advertising use.

Each processing purpose requires a valid basis where Applicable Law requires one. Optional consent must be freely given and capable of withdrawal. A general reference to legitimate interests does not replace consent where a particular disclosure or communications channel requires consent.

C.4 Disclosure to brokers and independent use

Where lawfully authorized, Everyday may disclose an eligible contact's name, email address or telephone number to a broker directly, or indirectly by entering, synchronizing or contributing the contact to a broker-operated list or service whose applicable arrangements permit independent use. The recipient may then use permitted information for its own advertising and marketing or that of others, subject to the recipient's obligations and the permissions governing the disclosure.

Such a transfer may constitute a sale of Personal Information, sharing for cross-context behavioral advertising, or another regulated disclosure depending on the jurisdiction and actual arrangement, even if Everyday does not receive money. Everyday must assess the actual transfer and provide required notice, consent or opt-out mechanisms. Labeling a transfer "non-direct" does not make it exempt.

Hosting a list and contributing information to a broker's independent database are different activities. Everyday must not enable independent reuse merely because a provider has the technical ability to store a contact. If the applicable agreement limits a provider to processing solely for Everyday, the provider must remain within that limitation unless a separate lawful disclosure is made.

This Schedule does not assert that every contact uploaded to Salesgenie or every contact obtained from ZoomInfo is automatically reused by that company. The relevant product arrangement and actual disclosure determine that issue. Everyday must not describe an uncertain independent-use arrangement as anonymous processing or as a processor-only relationship without a basis for doing so.

C.5 Broker policies and Everyday's responsibility

Salesgenie's privacy policy is available at Salesgenie / Data Axle Privacy Policy. ZoomInfo's privacy information is available through ZoomInfo Privacy Policy. These sources explain the brokers' independent practices and request channels; their policies may change.

Everyday does not control a broker's independent database or promise to erase every record a broker acquired separately. Nevertheless, Everyday remains responsible for its own decisions to obtain, use, contribute or disclose contact information, for required diligence about its source and permissions, and for requests and notifications Applicable Law requires Everyday to handle. Directing a person to a broker does not relieve Everyday of those duties.

Before using a broker record for a channel requiring permission, Everyday must have sufficient evidence of the relevant authorization, including its scope and the person or seller it covers. A broker's general privacy policy or a statement that a list is "compliant" does not by itself prove that a specific person authorized Everyday's automated marketing call or text.

C.6 Email, automated text and robocall marketing

Email. Everyday may send marketing email only where lawful, using accurate sender and subject information, appropriate identification of the commercial message, its valid postal address and a clear means to unsubscribe. A request to stop marketing email will be honored within the legally required period and no later than 10 business days after receipt. Where prior consent is required, Everyday must obtain it before sending.

Automated texts and artificial-voice or prerecorded calls. Everyday will obtain and retain separate, affirmative written permission sufficient for the relevant technology and jurisdiction before initiating these marketing channels. Its permission process must identify Everyday, the recipient's authorized telephone number, the marketing purpose and the relevant automated or artificial/prerecorded technology. Electronic consent may be used where legally valid. A person must not be required to consent as a condition of purchasing or using the API Service.

Channel boundaries. The required API acceptance checkbox is not the marketing consent mechanism. An existing customer relationship or inclusion on a purchased contact list does not replace the required permission. Consent for Everyday's communications does not automatically authorize a broker or another seller to make its own automated marketing calls or texts. Everyday must observe applicable do-not-call restrictions, recipient-local calling hours and state or international rules that are more protective.

Message controls. Marketing texts must provide a workable way to stop further messages; where replies are supported, a reply of STOP or another clear equivalent must be honored. Prerecorded marketing calls must identify the responsible caller and provide the legally required interactive opt-out and callback mechanisms. A consent invitation or campaign must disclose relevant message frequency and possible message or data charges. Participation requires separate enrollment identifying the sender and the applicable campaign terms; accepting this Agreement alone does not enroll an individual.

C.7 Withdrawal, suppression and disclosure opt-out

A person may stop Everyday marketing by using an email unsubscribe link, replying STOP or another clear refusal to a reply-enabled marketing text, using a call's opt-out function, submitting the form in Schedule D, or emailing support@everydaytrack.org. Everyday will accept another reasonable revocation method where law requires it. The Google form is an additional channel, not the exclusive way to revoke consent.

Everyday will implement a marketing revocation within a reasonable period, no later than 10 business days after receipt, and sooner where required. Full deletion from a broker-hosted list or a broker's independent system must not delay suppression of Everyday's further marketing. A processing estimate displayed on a form does not extend a statutory deadline.

A person may separately request that Everyday stop selling or sharing their contact information or stop disclosing it to brokers for independent advertising. Everyday will honor legally applicable opt-outs, including recognized universal opt-out signals such as Global Privacy Control where they apply. Consent required for a particular disclosure must be obtained before it occurs; an opt-out offered later does not cure the absence of required consent.

Everyday may retain a minimal suppression record to prevent further contact, disclosure or reimport. Suppression records are for honoring choices and compliance, not renewed advertising. A person need not pay, create a new account or provide unnecessary identification to stop marketing. Withdrawal does not affect processing that was lawful before withdrawal, but continued use must have an adequate independent basis.

C.8 Other privacy rights and request handling

Depending on Applicable Law, a person may request access, correction, deletion or portability; restrict or object to processing; withdraw consent; opt out of regulated sale, sharing or targeted advertising; or appeal a denial. Everyday will respond within the period applicable to the request and explain permitted extensions or exceptions when required. A form's reference to 1-7 weeks does not override a shorter response or suppression requirement.

Everyday may verify identity and authority proportionately for access or deletion, especially where disclosure could expose another person's information. It will not require the same verification for a simple marketing opt-out where that would be unnecessary or unlawful. An authorized agent may act where permitted, subject to appropriate proof of authority. An appeal may be emailed with the subject "Privacy Request Appeal."

Where legally required, Everyday will communicate a deletion or disclosure opt-out to relevant recipients and processors. A broker that independently controls information may also need to receive a direct request through its own policy. Everyday will explain that distinction without making a direct broker request a condition of honoring the portion within Everyday's responsibility.

Everyday will not unlawfully discriminate against a person for exercising a privacy right. A person may complain to the competent privacy or consumer-protection authority. Choosing not to receive marketing does not remove the ability to receive necessary account-security, billing or service notices; those notices must not be used as a pretext to resume advertising.

C.9 Retention and sensitive audiences

Marketing records may remain after API cancellation while a lawful marketing purpose and required permission continue, subject to suppression, deletion rights and periodic review of necessity. Account cancellation does not make marketing consent permanent, and silence does not justify indefinite retention. Permission evidence and minimal suppression records may be retained as necessary to demonstrate compliance and avoid repeat contact.

Everyday will not knowingly use these broker-marketing activities to target children under 18 or disclose their contact information for independent broker advertising. It will not intentionally collect sensitive-category information for this program. Information learned to be subject to additional restrictions must be excluded or handled with the safeguards and permissions required by Applicable Law.

Material changes to categories, purposes or independent recipients require appropriate updated notice and, where necessary, fresh consent before the changed processing. The API agreement cannot be used to retroactively turn a limited support or consumer-account disclosure into unrestricted permission for advertising.

Schedule D. Requests, contacts and policy directory

D.1 Responsible provider and postal notices

Jameson E Jones, doing business as Everyday Track
Sole proprietorship; operating under the Everyday brand
6339 Charlotte Pike, PMB 2015
Nashville, TN 37209
United States
Website: everydaytrack.org
Email: support@everydaytrack.org

The mailing address may be used for legal and privacy correspondence. It is a mailing address and does not represent a walk-in customer-support location. Include enough information to identify the request; do not include a complete active API key, password or unnecessary sensitive information.

D.2 Online request form and email alternative

Use the Everyday opt-out and deletion request form to request the available account and broker-list actions. The form is hosted by Google and information submitted through it is also handled through Google's systems. If the form is unavailable, does not identify the relevant account or contact, or does not offer the requested action, email support@everydaytrack.org instead. A Google account is not required to use the email alternative.

State the action requested and the email address, phone number or account identifier to which it applies. Everyday may request appropriate follow-up information where needed to find a record or verify an access or deletion request. It will not require unnecessary verification to process a clear marketing revocation. Requests remain valid if they use different wording or another method protected by law.

D.3 Recommended email subjects

API Support - integration questions and documented API behavior.
API Billing - charges, renewals and payment corrections.
API Cancellation - stop renewal or close API access.
API Availability Credit - request review under Schedule A.
API Security Incident - compromised keys or suspected unauthorized access.
API Legal Dispute - legal correspondence and informal dispute notice.
API Agreement Copy - request this Agreement or available acceptance records.
Privacy Request - Access / Correction / Deletion - identify the applicable action.
Marketing Opt-Out - stop Everyday advertising communications.
Do Not Sell or Share / Broker Disclosure Opt-Out - stop covered independent advertising disclosures.
Privacy Request Appeal - request review of a privacy decision.

These subjects are routing recommendations, not mandatory formalities. An ordinary, understandable request will not be rejected solely because a subject line differs. Cancelling access, stopping marketing, opting out of disclosure and deleting information can be requested together, but they have the distinct effects explained in this Agreement.

D.4 Policy directory

Everyday website Terms of Service and Privacy Policy govern their stated scope. Track123 Terms of Service and Track123 Privacy Policy describe relevant general provider terms. TrackingMore Terms of Service provide the published provider terms or their current redirected location. A separate applicable upstream agreement may supplement those public terms.

Salesgenie / Data Axle Privacy Policy and ZoomInfo Privacy Policy describe the brokers' independent practices and request options. These links are informational and do not grant Everyday or Customer a right withheld by the relevant provider. A link changing location does not expand a license or remove an obligation under this Agreement.

D.5 Acceptance record

By affirmatively selecting the required API signup checkbox linked to this Agreement, Customer accepts Version 1.0 as the applicable API contract, subject to the scope and effective-date provisions in Section 1. The accepting Customer is identified by the associated account and acceptance record, rather than by a blank signature field in this published document. Optional marketing permissions, where given, must be separately recorded as described in Schedule C.