

Privacy Notice — B2B Website and Platform

Last updated: Sep 23, 2026

1. Scope

This Privacy Notice explains how Nowcasting.ai, Inc. ("Streetbeat," "we," "us," or "our") collects, uses, discloses, and retains personal information in connection with:

- The Streetbeat business-to-business website.
- Requests for demonstrations, information, or other communications.
- Business relationships with prospective and existing enterprise customers.
- Authorized use of the Streetbeat enterprise platform.

This notice does not apply to the Streetbeat consumer investment application, which is governed by its own privacy policy, or to job applicants, whose information is governed by the separate Applicant Privacy Notice.

Customer data processed through the enterprise platform is also governed by the applicable Master Services Agreement, Data Processing Addendum, and related customer instructions. If those documents conflict with this notice concerning customer data, the contractual documents control.

2. Who is responsible for your information

Nowcasting.ai, Inc. 1000 N. West Street, Suite 1200 Wilmington, DE 19801, United States

Privacy inquiries and requests may be sent to privacy@streetbeat.com, which is handled by our Privacy Team.

Nowcasting.ai, Inc. may work with its affiliates where their personnel, infrastructure, or services support the website, platform, or business relationship.

For European and UK data-protection purposes, Nowcasting.ai, Inc. acts as controller of the business-contact, website, account-administration, and similar information described in this notice.

When Streetbeat processes personal information supplied by an enterprise customer through the platform solely on that customer's documented instructions, the customer generally acts as controller or business and Streetbeat acts as processor or service provider. The applicable customer agreement determines the parties' specific roles.

3. Information we collect

Information you provide

- Name and business contact information.
- Employer, job title, department, and professional role.
- Information included in a demo request, contact form, questionnaire, email, or meeting.
- Account-administration information for authorized platform users.
- Support requests, communications, and troubleshooting information.
- Marketing and communication preferences.
- Information supplied in connection with due diligence, procurement, security review, or contract administration.

Website and technical information

- Browser, device, and approximate-location information derived from an IP address.
- Pages viewed, referral information, interaction events, and similar website analytics.
- Cookie and consent information.
- Security, authentication, access, API, diagnostic, error, and service-performance logs.

Nonessential website technologies are used only after consent where consent is legally required. Additional information appears in the Cookie Notice.

Information received from other sources

We may receive professional contact information from your employer or colleagues, business partners and referrals, professional networking platforms (e.g., LinkedIn), event organizers, publicly available professional sources, and service providers that support business development or data accuracy. We may also obtain professional contact information (name, job title, company, business email) from business-contact data providers. When legally required, we will provide additional notice when we obtain personal information from another source, including in our first communication with you.

Sensitive personal information

We do not request or intentionally process sensitive personal information (such as information about health, racial or ethnic origin, religious or philosophical beliefs, political opinions, trade-union membership, sex life or sexual orientation, biometric or genetic data, or government identification numbers) through the website, our business-development activities, or platform administration. Please do not send us such information.

Customer data — platform

Streetbeat provides an AI-powered software platform licensed to enterprise clients. Streetbeat operates under a strict principle of no intentional access to personal data belonging to our clients' customers or users. If any such access occurs, it is purely accidental, non-systematic, and limited to what a client may voluntarily expose during a support or troubleshooting interaction; such data is not retained, is promptly deleted or irreversibly removed, and is never used for any independent purpose.

In normal operation Streetbeat processes only: (1) Business Contact Information of client representatives, for account setup/administration, support, and contractual/operational correspondence; and (2) Technical Metadata (system logs, API metadata, diagnostics, error information), for operating and securing the service, incident response, troubleshooting on client request, and performance/reliability. Streetbeat does not use technical metadata for profiling, marketing, advertising, or analytics unrelated to service performance.

Enterprise customers determine what information they submit to the platform and are responsible for ensuring they have a legal basis and authority to provide it.

4. How we use information

Primary purposes — necessary for the relationship you have or request with us. We may use personal information to: operate the B2B website; respond to inquiries and arrange demonstrations; contact you in your professional capacity to present our B2B solutions; evaluate and manage prospective and existing business relationships; negotiate and administer contracts; create and manage authorized platform accounts; provide, maintain, secure, monitor, and support the platform; authenticate users and prevent unauthorized access; diagnose errors and address support requests; communicate about service, security, contractual, and operational matters; conduct internal reporting and product planning using aggregated or de-identified information; protect our personnel, customers, services, systems, and legal rights; detect, investigate, and prevent fraud, abuse, security incidents, and unlawful activity; comply with legal, regulatory, accounting, and recordkeeping requirements; establish, exercise, or defend legal claims; and complete a merger, financing, acquisition, reorganization, sale, or similar corporate transaction.

Secondary purposes — not necessary for the relationship: commercial prospecting, marketing, and communications about our products, services, and events; and measuring website and communication performance. You may refuse or object to these secondary purposes at any time, free of charge, by replying to our email, writing to privacy@streetbeat.com, or using the unsubscribe link where the message includes one. Refusing them does not affect the primary purposes.

Streetbeat does not use customer data to train shared or general-purpose artificial-intelligence models unless the applicable customer has expressly agreed in writing.

5. Legal bases in the EEA and UK

Where the GDPR or UK GDPR applies, we rely on:

- Contract and requested pre-contractual steps — to respond to a requested demonstration, administer a customer relationship, provide contracted services, and support authorized users.
- Legitimate interests — to develop business relationships, operate and improve the website and platform, maintain security, prevent fraud, perform

limited business analytics, and protect legal rights, assessed against individual rights.

- Consent — for nonessential cookies and similar technologies and for communications or other processing where consent is required; consent may be withdrawn at any time.
- Legal obligations — to comply with applicable laws, lawful requests, accounting requirements, and regulatory obligations.
- Legal claims — to establish, exercise, or defend claims where applicable law permits.

6. How we disclose information

We may disclose personal information to: Streetbeat personnel with a business need to know; our affiliates where they support the relevant activity; hosting, cloud, communications, analytics, CRM, security, support, and professional-service providers; enterprise customers that administer their own authorized users; auditors, insurers, lawyers, accountants, and other professional advisers; courts, regulators, law-enforcement bodies, and government authorities when required or permitted by law; parties involved in a proposed or completed corporate transaction, subject to appropriate safeguards; and other recipients at your direction.

Service providers are contractually restricted from using personal information for purposes unrelated to the services they provide to Streetbeat.

Accountability for onward transfers (EU-U.S. DPF). When Streetbeat transfers personal data received in reliance on the EU-U.S. DPF to third-party agents or service providers acting on our behalf, we require that they provide at least the same level of protection as required by the DPF Principles. Streetbeat remains liable under the DPF Principles if such an agent processes the data in a manner inconsistent with the Principles, unless Streetbeat proves it is not responsible for the event giving rise to the damage.

Streetbeat does not sell personal information for monetary consideration and does not share B2B website personal information for cross-context behavioral advertising.

7. International transfers

Streetbeat is located in the United States, and personal information may be processed in the United States, in Italy (where one of our affiliates is established), and in other countries where Streetbeat, its affiliates, customers, or service providers operate.

For personal data transferred from the EU/EEA, Streetbeat relies on the EU-U.S. Data Privacy Framework (EU-U.S. DPF) as its primary transfer mechanism (see Section 8), and additionally, or as a fallback, on the European Commission's Standard Contractual Clauses (SCCs).

You may contact privacy@streetbeat.com for information about applicable transfer safeguards.

8. EU-U.S. Data Privacy Framework

Nowcasting.ai, Inc. complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) as set forth by the U.S. Department of Commerce. Nowcasting.ai, Inc. has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. DPF Principles with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF. If there is any conflict between the terms of this notice and the EU-U.S. DPF Principles, the Principles govern. To learn more about the DPF program and to view our certification, visit <https://www.dataprivacyframework.gov/>.

Choice. In accordance with the DPF, you may limit the use and disclosure of your personal data. Specifically, you may opt out of (i) disclosure of your personal data to third parties not acting as agents on our behalf, and (ii) use of your personal data for a purpose materially different from that for which it was originally collected or subsequently authorized. To exercise these choices, contact privacy@streetbeat.com.

FTC. Nowcasting.ai, Inc. is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC) with respect to its compliance with the EU-U.S. DPF.

Recourse. See Section 15 (Your rights) and Section 18 (Contact) for the independent recourse mechanism, the EU DPA panel, and binding arbitration available under the DPF.

9. Retention

Streetbeat retains personal information only as long as reasonably necessary:

- Demo requests and prospective-customer records: up to 24 months after the last substantive interaction.
- Customer account and contract-administration records: for the customer relationship and up to seven years afterward where needed for legal, tax, accounting, or claims purposes.
- Platform security and diagnostic logs: ordinarily up to 12 months unless a different period is required by contract, security needs, or law.
- Support communications: ordinarily up to three years after closure.
- Marketing contact information: until you opt out or after 24 months without a substantive business interaction.
- Cookie and consent records: for the periods shown in the Cookie Notice and Cookiebot declaration.

Information may be retained longer for litigation holds, investigations, security incidents, legal obligations, or the establishment, exercise, or defense of legal claims. When retention is no longer necessary, we delete, anonymize, or securely isolate the information.

10. Security

Streetbeat uses administrative, technical, and organizational safeguards designed to protect personal information, which may include access controls, least-privilege practices, encryption in transit and at rest where appropriate, monitoring, logging, network isolation, secure-development practices, and incident-response procedures. No method of transmission or storage is completely secure, and Streetbeat cannot guarantee absolute security.

11. Marketing communications

You may opt out of marketing emails by replying to the email, by contacting privacy@streetbeat.com, or by using the unsubscribe link where the message includes one. We keep a suppression list of individuals who have opted out; registration is free of charge and we confirm it to you by email. Opting out does not prevent necessary service, security, contractual, or transactional communications.

12. Cookies

Streetbeat uses Cookiebot to provide information about cookies and manage consent. Where required, nonessential cookies remain disabled until permission is provided. You may change or withdraw your choice through the Cookie Settings control in the website footer. See the Cookie Notice for details.

13. California and other U.S. state notices

Streetbeat may collect these categories from B2B website visitors and enterprise contacts: identifiers and business contact information; professional and employment-related information; internet or electronic-network activity; approximate geolocation derived from an IP address; commercial and customer-relationship information; communications and support records; and inferences concerning business interests or likely product needs.

Streetbeat uses and retains these categories for the purposes and periods described in this notice and may disclose them to the recipient categories described above. Streetbeat does not sell this information for monetary consideration or share it for cross-context behavioral advertising. Residents of states that provide applicable privacy rights may request access, correction, deletion, or a copy, and may appeal certain decisions, by contacting privacy@streetbeat.com.

14. Automated decision-making

Streetbeat does not use B2B website information to make decisions that produce legal or similarly significant effects solely through automated processing. If this changes, Streetbeat will provide the notice and choices required by applicable law.

15. Your choices and rights

Depending on your location and applicable law, you may have the right to: request access; request correction; request deletion; request restriction; object to processing based on legitimate interests; object to direct marketing; receive certain information in a portable format; withdraw consent; appeal our response

where applicable; lodge a complaint with a privacy or data-protection authority; and exercise your rights without unlawful discrimination or retaliation.

To exercise a right, contact privacy@streetbeat.com. We may request information necessary to verify your identity and authority. Authorized agents may submit requests where permitted by law.

We respond free of charge and within the time limits set by applicable law — for example, one month under the GDPR (extendable where the law allows), 45 days under California law, and 20 days to respond plus 15 days to give effect under Mexican law. If we need more time or cannot fulfil a request, we will tell you why.

Individuals in the EEA or UK may also lodge a complaint with the data-protection authority where they live or work or where they believe a violation occurred.

16. Children

The B2B website and enterprise platform are not directed to children, and Streetbeat does not knowingly collect personal information from children through these services.

17. Changes to this notice

Streetbeat may update this notice to reflect changes in its practices, services, or legal obligations, posting the updated notice at this same URL with a revised “Last updated” date. Where legally required, Streetbeat will provide additional notice of material changes, and if the purposes of processing change we will notify you by email.

18. Contact and DPF recourse

Nowcasting.ai, Inc. 1000 N. West Street, Suite 1200 Wilmington, DE 19801, United States Email: privacy@streetbeat.com

EU-U.S. DPF complaints. In compliance with the EU-U.S. DPF, Nowcasting.ai, Inc. commits to resolve DPF Principles-related complaints about our collection and use of your personal information. EU individuals with inquiries or complaints should first contact us at privacy@streetbeat.com.

Nowcasting.ai, Inc. commits to cooperate and comply with the advice of the panel established by the EU data protection authorities (DPAs) with regard to unresolved complaints concerning personal data received in reliance on the EU-U.S. DPF.

Binding arbitration. Under certain conditions and as a last resort, EU individuals may invoke binding arbitration to resolve complaints regarding Streetbeat's compliance with the EU-U.S. DPF Principles, after (i) raising the concern directly with Streetbeat, (ii) using the EU DPA panel recourse mechanism, and (iii) raising the matter with the U.S. Department of Commerce. If the complaint remains unresolved, the individual may invoke binding arbitration by delivering written notice to Streetbeat, following the procedures in Annex I of the EU-U.S. DPF Principles. Streetbeat is obligated to arbitrate claims subject to the terms of Annex I.

19. Individuals in Mexico

If you are located in Mexico, our Aviso de Privacidad Integral (in Spanish), available at https://streetbeat.com/docs/Streetbeat_Aviso_Privacidad_Mexico.pdf, applies in addition to this notice and describes how to exercise your ARCO rights (access, rectification, cancellation and objection) under the Ley Federal de Protección de Datos Personales en Posesión de los Particulares. In case of discrepancy for individuals in Mexico, the Aviso de Privacidad prevails.