

TERMS OF SERVICE

Bot Pulse API Platform

Version 1.1 — Effective Date: 1.2.2026

1. Definitions

1.1 API: The application programming interface(s) — including solver, TLS proxy, and related services — developed and offered by Provider on the Platform under these Terms, together with all corresponding Documentation.

1.2 Credentials: API keys, tokens, usernames, passwords, and any other access credentials enabling use of the Platform and API.

1.3 Documentation: Technical content, integration guides, API references, and acceptable use specifications published by Provider.

1.4 Enterprise Agreement: A separate written Master Service Agreement (MSA) between Provider and an enterprise User, which supplements or supersedes these Terms where expressly stated.

1.5 Force Majeure: Events outside Provider's reasonable control, including war, natural disasters, government action, internet infrastructure failure, third-party WAF vendor updates, cyberattacks, electricity failure, third-party service failure, strikes, or pandemics.

1.6 GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council.

1.7 Intellectual Property: All intellectual property rights, whether registered or unregistered, including patents, copyrights, database rights, trademarks, trade secrets, and know-how.

1.8 Platform: The online platform at botpulse.io through which Provider makes the API available.

1.9 Solved Token / Token: One successfully resolved WAF or antibot challenge as delivered by the API. Failed solves are not billed.

1.10 SLA: The service availability and remedy terms set out in clause 7 of these Terms, or as agreed in an Enterprise Agreement.

1.11 User / Customer: The legal entity or individual that registers an account on the Platform and accesses the API.

1.12 User Data: Data transmitted through the API by the User or generated as a result of API use, excluding anonymized analytics and server log files.

1.13 WAF Vendor Update: A change, patch, or update deployed by a third-party web application firewall or antibot vendor that affects the availability or success rate of the API's solver functionality.

2. General

2.1 These Terms govern access to and use of the Platform and API. By registering an account or accessing the API, the User accepts these Terms in full.

2.2 Where a User has executed an Enterprise Agreement with Provider, the Enterprise Agreement governs to the extent of any conflict with these Terms.

2.3 Provider may amend these Terms at any time. For pay-as-you-go Users, amendments take effect no earlier than thirty (30) days after notice is provided via email or Platform notification. For Users with active committed-volume subscriptions (annual or multi-year), Provider will provide at least sixty (60) days' written notice of any material changes affecting pricing, liability, or service scope. Continued use after the effective date constitutes acceptance.

2.4 If any provision is held invalid or unenforceable, the remaining provisions continue in full force. Provider will replace invalid provisions with valid provisions reflecting the original intent.

2.5 These Terms are drawn for the benefit of Provider, its affiliates, directors, employees, and third parties engaged in connection with the API, as a third-party clause under applicable law.

3. Right to Use the API and Platform

3.1 Subject to the User's payment obligations and compliance with these Terms, Provider grants the User a limited, personal, revocable, non-exclusive, non-transferable license to access and use the API for the User's own internal business purposes.

3.2 The User may not, directly or indirectly:

- Use the API for any purpose that violates applicable law or regulation in the User's jurisdiction or the jurisdiction of the target;
- Resell, sublicense, redistribute, or offer the API as a standalone service to third parties without a separate written white-label or reseller agreement with Provider;
- Copy, reverse engineer, decompile, disassemble, or otherwise attempt to derive source code from the API or Platform;
- Remove or alter proprietary notices, labels, or credits from the API or Platform;
- Interfere with, circumvent, or attempt to disable the security or access control features of the API or Platform;
- Use the API in a manner that causes material damage to the API, Platform, or Provider's infrastructure;
- Share Credentials with third parties outside the User's organization without prior written consent from Provider.

3.3 Provider may monitor API usage to ensure quality, verify compliance, and improve services. The User shall not interfere with such monitoring.

3.4 Provider may suspend access immediately and without prior notice if Provider reasonably believes the User is in material violation of these Terms, applicable law, or the Acceptable Use Policy. Provider will provide written notice of suspension promptly after the fact and will allow the User a reasonable opportunity to cure non-material violations before termination.

4. Acceptable Use Policy

4.1 The API is designed to assist organizations with legitimate data access, price intelligence, and web automation use cases. Permitted uses include travel data aggregation, price monitoring, competitive intelligence, and integration testing against targets the User has authorization to access.

4.2 The following use is strictly prohibited:

- Using the API as part of a fraud or phishing operation, including facilitating unauthorized access to third-party accounts or systems through deceptive means.

4.3 Provider reserves the right to update the Acceptable Use Policy by providing thirty (30) days' notice. Users who do not accept updated AUP terms may terminate their subscription and receive a pro-rata refund of unused committed fees.

5. Accounts, Credentials, and Organization Access

5.1 Users must register an account by providing accurate, complete, and current information. Provider may reject or remove accounts at its discretion in cases of duplicate accounts, suspected fraud, or AUP violations.

5.2 The User is solely responsible for maintaining the confidentiality of its Credentials and for all activities conducted under its account. The User must notify Provider immediately upon becoming aware of any unauthorized use or security breach.

5.3 Enterprise Users may create sub-accounts for individual team members within their organization ("Organization Access"). This allows a single enterprise account with shared billing and usage visibility, while each team member operates under their own API key. The enterprise account holder is responsible for ensuring all sub-users comply with these Terms. Provider may share account-level usage data with the enterprise account holder for billing allocation and compliance purposes. Sub-user access may be granted, modified, or revoked by the enterprise account holder at any time via the Platform dashboard.

5.4 Users must not disclose Credentials to third parties outside their organization. Credential sharing for commercial purposes without a reseller agreement constitutes a material breach of these Terms.

6. Fees, Billing, and Payment

6.1 Provider offers the following payment models: pay-as-you-go (balance credits pre-loaded to the User's account) and committed volume subscriptions (monthly, annual, or multi-year). Pricing is as published on the Platform or as agreed in an Enterprise Agreement.

6.2 Fees are payable in advance and are non-refundable except as set out in clause 6.6 and clause 8.

6.3 Subscriptions automatically renew until terminated in accordance with clause 8. The User may terminate a subscription before the renewal date to prevent renewal billing.

6.4 Pay-as-you-go balance credits are valid for twelve (12) months from the date of purchase. Credits do not carry cash value and are non-transferable. Unused credits expire upon account closure.

6.5 Fee changes are governed as follows: (a) for pay-as-you-go and month-to-month subscriptions, Provider may change fees at any time with thirty (30) days' written notice; (b) for committed annual or multi-year subscriptions, the contracted price is locked for the duration of the subscription period and may not be increased by Provider during that period. Updated fees apply only upon renewal.

6.6 Failed solves — where the API does not return a successfully resolved token — are not billed. Retries within the same session window as defined in the Documentation are included in the original token cost.

7. Service Levels and Solver Availability

7.1 Provider will use commercially reasonable efforts to maintain API availability. However, given the nature of WAF and antibot technologies, Provider cannot guarantee uninterrupted solver availability. Solver functionality may be temporarily degraded or unavailable following a WAF Vendor Update while Provider develops and deploys an updated solver response.

7.2 WAF Vendor Update remedy: In the event of solver unavailability directly caused by a WAF Vendor Update, Provider will extend the expiry of affected prepaid tokens by a period equal to the documented downtime. This token expiry extension is the User's sole remedy for downtime caused by WAF Vendor Updates.

7.3 For downtime caused by Provider infrastructure failure (not attributable to a WAF Vendor Update), Provider will also extend affected token expiry by the documented downtime period. Enterprise Agreements may specify additional remedies including service credits.

7.4 Scheduled maintenance will be communicated with at least 48 hours' advance notice except in cases of emergency. Scheduled maintenance windows do not qualify for token expiry extension.

7.5 Enterprise Users may negotiate enhanced service level terms — including dedicated infrastructure, priority incident response, and financial remedies — through an Enterprise Agreement.

8. Term and Termination

8.1 These Terms take effect when the User first accesses the Platform and remain in force until terminated.

8.2 Pay-as-you-go and month-to-month Users may terminate their account at any time with immediate effect. No refund is due for unused balance credits on pay-as-you-go accounts, except where termination is due to Provider's material breach.

8.3 Users on committed annual or multi-year subscriptions may terminate by providing written notice to Provider. Termination takes effect at the end of the then-current subscription period. Where Provider terminates a committed subscription for reasons other than the User's breach or AUP violation, Provider will issue a pro-rata refund of prepaid fees for the unused portion of the subscription period.

8.4 Provider may terminate these Terms for cause immediately upon written notice if the User: (a) materially breaches these Terms and fails to cure within fifteen (15) days of notice; (b) violates the AUP; (c) becomes insolvent or subject to insolvency proceedings; or (d) uses the API in a manner that creates material legal, regulatory, or reputational risk for Provider.

8.5 Upon termination: (a) access to the Platform and API ceases immediately; (b) the User's Credentials are revoked; (c) refunds are issued in accordance with clauses 8.2 and 8.3 above.

9. Confidentiality

9.1 Each party agrees to maintain as confidential all non-public information disclosed by the other party in connection with these Terms that is designated as confidential or that reasonably should be understood to be confidential given the nature of the information ("Confidential Information").

9.2 Provider will treat as confidential: (a) the User's API usage patterns and volumes; (b) the User's technical integration details; (c) any business information shared by the User in the context of an Enterprise Agreement.

9.3 The User will treat as confidential: (a) the API's technical implementation details; (b) Provider's pricing other than publicly published rates; (c) any non-public product roadmap or technical specifications shared by Provider.

9.4 Confidentiality obligations do not apply to information that: (a) is or becomes publicly known through no breach of this clause; (b) was already known to the receiving party without restriction; (c) is required to be disclosed by applicable law or court order, provided the disclosing party is given prompt notice where legally permitted.

9.5 Confidentiality obligations survive termination of these Terms for a period of three (3) years.

10. Intellectual Property

10.1 All Intellectual Property rights in and related to the API, Platform, and underlying technology vest exclusively in Provider or its licensors. The User acquires only the limited usage rights expressly granted in these Terms.

10.2 The User retains all Intellectual Property rights in User Data. The User grants Provider a limited, non-exclusive license to process User Data solely to the extent necessary to provide the API.

10.3 Provider does not claim ownership over the outputs of the API (solved tokens, proxy responses) delivered to the User.

10.4 The User is prohibited from removing or altering any proprietary notices or credits from the Platform or API.

11. Data Processing and Privacy

11.1 Provider processes personal data about Users (account and billing data) as a data controller, as described in the Privacy Policy at botpulse.io/privacy.

11.2 To the extent Provider processes personal data on behalf of the User in connection with the API (acting as a data processor), the parties will execute a Data Processing Agreement (DPA) as required under GDPR or other applicable data protection law. Provider's standard DPA is available on request at contact@botpulse.io.

11.3 User Data transmitted through the API is processed solely to provide the service and is not retained beyond what is necessary for service delivery, security, and compliance purposes.

12. Limitation of Liability

12.1 Provider's total aggregate liability to the User under or in connection with these Terms — whether in contract, tort (including negligence), or otherwise — shall not exceed the lower of: (a) the total fees paid by the User to Provider in the six (6) months preceding the event giving rise to the claim; or (b) USD 5,000.

12.2 Provider shall not be liable for: indirect, consequential, special, incidental, or punitive loss or damage; loss of profit; loss of revenue; loss of data; loss of business opportunity; or reputational harm, even if Provider has been advised of the possibility of such loss.

12.3 The limitations in clauses 12.1 and 12.2 do not apply to: (a) liability for death or personal injury caused by Provider's negligence; (b) liability for fraud or fraudulent misrepresentation; (c) any liability

that cannot be limited by applicable law.

12.4 Provider shall not be liable for solver unavailability or degraded success rates caused by WAF Vendor Updates, which constitute Force Majeure events for the purposes of these Terms.

12.5 Provider shall not be liable for failure to perform obligations caused by other Force Majeure events.

12.6 A condition for any claim is that the User notifies Provider in writing within thirty (30) days of becoming aware of the event giving rise to the claim. Claims lapse twelve (12) months after the date of the relevant event.

13. Indemnification

13.1 The User will indemnify, defend, and hold harmless Provider and its officers, directors, employees, and contractors from and against any claims, damages, losses, and costs (including reasonable legal fees) arising from or related to: (a) the User's breach of these Terms; (b) the User's violation of applicable law; (c) the User's misuse of the API; or (d) any third-party claim arising from User Data.

14. Governing Law and Dispute Resolution

14.1 These Terms are governed by and construed in accordance with the laws of England and Wales, without regard to conflict of law principles.

14.2 Any dispute arising out of or in connection with these Terms that cannot be resolved by good-faith negotiation within thirty (30) days shall be submitted to the exclusive jurisdiction of the courts of England and Wales.

14.3 Enterprise Users may agree to alternative dispute resolution mechanisms including arbitration in their Enterprise Agreement.

15. General Provisions

15.1 These Terms, together with any Enterprise Agreement, DPA, and the Privacy Policy, constitute the entire agreement between the parties regarding the subject matter herein and supersede all prior agreements.

15.2 Provider's failure to enforce any provision of these Terms does not constitute a waiver of that provision.

15.3 The User may not assign or transfer its rights or obligations under these Terms without Provider's prior written consent. Provider may assign its rights and obligations to an affiliate or in connection with a merger, acquisition, or sale of assets.

15.4 Notices under these Terms must be in writing and delivered by email to the address on file or to contact@botpulse.io.

botpulse.io

Dubai, UAE

Contact: contact@botpulse.io

Platform: <https://botpulse.io>

Version 1.1 — 1.2.2026. This document supersedes all prior versions.