

Brandwatch Service Appendix – last updated: 5 September 2025

This Brandwatch Service Appendix (“Appendix”) which may also be referred to as the “Social Listening Service Appendix” or “Social Media Management Service Appendix” supplements the existing agreement in place between the parties (“Master Agreement”). Capitalized terms used but not defined in this Appendix have the meanings given in the Master Agreement. In the event of any conflict between this Appendix and the Master Agreement, this Appendix prevails.

1. Definitions

“**Deliverable**” means customised work from Supplier’s research team created for Customer.

“**Influence Help Center**” means the documentation at <https://intercom.help/paladin-software/en/>.

“**Influence Services**” means influencer discovery, Influence CRM, and campaign management services that Supplier provides to Customer.

“**Report**” means a customised report from Supplier’s research team created for Customer.

“**Services**” means the social listening, social media management and customer engagement services, and Influence Services that Supplier provides to Customer.

“**Suite Help Center**” means the documentation at <https://social-media-management-help.brandwatch.com/hc/en-us>.

“**Third-Party Services**” means services that are not provided by Supplier but that Customer may access or use in connection with the Services including social networks.

2. Service terms

2.1 Responsibility. Customer will comply with the X, (formerly Twitter), Terms of Service, usually at <https://twitter.com/tos>, the YouTube Terms of Service, usually at <https://www.youtube.com/t/terms>, the Meta (formerly Facebook), Terms of Service, usually at <https://www.facebook.com/terms.php>, and the WhatsApp Business Solution Terms, usually at <https://www.whatsapp.com/legal/business-solution-terms>, and the Reddit User Agreement, usually at <https://www.redditinc.com/policies/user-agreement>, as applicable, or such other terms that Customer has entered into with an applicable social data provider directly.

2.2 Third-Party Services. Customer’s use of Third-Party Services and access to data from Third-Party Services is governed by the applicable terms and policies of the third party provider. Supplier is only responsible for its own Services and not any Third-Party Services. Third-party sources may choose at any time to modify applicable restrictions or prohibit their content, features, or functionality from being accessed under this Agreement. If a Third-Party Service provider ceases to make a Third-Party Service available for use with certain features and functionality of the Services, Supplier will stop providing access to such features or functionality without liability. Fair usage limits apply to the number of accounts with Third-Party Services that Customer manages via the Services.

2.3 Use Case Approval. If a third-party content provider requires use case approval, Customer will not use such third-party content until Customer’s use case has been approved in writing and notified to Customer. Further, Customer’s continued use of the approved third-party content is subject to any changes or revocations of approval by the third-party content provider. Customer agrees to cease use of third-party content immediately if prior approval is subsequently modified, suspended, or revoked.

2.4 AI Usage. Customer will not, and will not allow any third party or sub-processor to, use Supplier Data to train, develop, enhance, or contribute to any generative artificial intelligence models, machine learning models, or any form of algorithmic or software-based artificial intelligence systems, without obtaining prior written consent from Supplier.

2.5 User protection. Customer will not: (a) knowingly display, distribute, or otherwise make Supplier Data available to any person or entity that it reasonably believes may use Supplier Data in a manner that would have the potential to be inconsistent with that individual's reasonable expectations of privacy; (b) conduct research or analysis that isolates a small group of individuals or any single individual for unlawful or discriminatory purposes; (c) use Supplier Data intending to cause harm, or to target, segment, or profile any individual based on health, negative financial status or condition, political affiliation or beliefs, racial or ethnic origin, religious or philosophical affiliation or beliefs, sex life or sexual orientation, trade union membership, data relating to any alleged or actual commission of a crime, or any other sensitive categories of personal information prohibited by Applicable Law; (d) without Supplier's prior written consent, but subject to Applicable Law, display, distribute, or otherwise make Supplier Data available to any member of the intelligence community or any other government or public-sector entity; or (e) use the Services to upload, store or transmit: (i) indecent or unlawful material; (ii) unsolicited communications; or (iii) material in violation of third-party privacy, publicity or intellectual property rights or any terms or conditions, policies or guidelines of any Third-Party Services.

2.6 Supplier Data. If Customer processes Supplier Data containing personal data, Customer is responsible for providing appropriate privacy notices to data subjects, including naming Supplier as a source of personal data. A licensor or Applicable Law may require Supplier to remove personal data within any Supplier Data. In such cases, Supplier will notify Customer of the impacted Supplier Data that requires removal and Customer will promptly remove such data from its systems, whether during or after the Term. Supplier Data is provided "as is", exclusive of any express or implied warranties.

2.7 Users. The Services may be used by the number of Users set out on an Order and may not be used by more than that number concurrently. Each User account is for 1 individual only and must not be shared between individuals. A generic User account (e.g. social@customer.com) is not a valid User account even if only used by 1 individual. Unless stated otherwise on an Order, Users must be employees, consultants, contractors or agents of the specific Customer entity identified on the Order.

2.8 Security. Customer will use commercially reasonable efforts to prevent unauthorised access to the Services or Supplier Data and will use security measures consistent with best industry standards to safeguard any Supplier Data downloaded to Customer's systems. Customer is responsible for determining whether to use any multi-factor authentication method beyond Supplier's default security settings. If Customer elects to use its own identity provider system ("IdP") to authenticate its Users, Customer will periodically review and ensure proper security of such IdP at Customer's expense. If Customer grants Supplier access to Customer Data via any web portal or other non-public websites or extranet services on Customer's or a third party's website or system, Customer is responsible for information security governance in connection with such access, including the management of user accounts and access rights.

2.9 Support. Customer support for the Services (excluding the Influence Services) will be provided as set out in the Help Center, except as otherwise described in this Appendix. Customer support for the Influence Services will be provided as set out in the Influence Help Center.

2.10 Customer may export Customer Data during the Term. After expiry of this Agreement or deprecation of an affected legacy platform, Supplier will have no obligation to store Customer Data, and Supplier will delete all copies of such data in the ordinary course of business, unless legally prohibited.

2.11 Updates. This Appendix may be updated periodically to cover product or technical developments, changes to law, or to include terms that content suppliers require. Notification of material changes will be delivered as required by law. Subject to the foregoing, continued use of these Services will constitute acceptance of these terms.

3. Intellectual property

3.1 Reports. Supplier owns any Report, excluding any Customer Data in a Report. Supplier grants to Customer a worldwide, non-exclusive, non-transferable, royalty-free licence to use the Report and the Supplier Data in the Report in accordance with the Agreement.

3.2. Supplier Data licence. Supplier grants to Customer a worldwide, non-exclusive, non-transferable, royalty-free, licence to use, download, copy, or otherwise remove Supplier Data from Supplier's systems, for use in accordance with the Agreement, during the Term. All rights not expressed granted to Customer herein are reserved to Supplier and its data licensors, as applicable.

3.3. Customer Data licence. Customer grants to Supplier a non-exclusive, royalty-free licence to process Customer Data for the purposes of providing the Services.

4. Benchmark Module terms

This section 4 only applies if Customer's Order includes access to benchmarking functionality ("Benchmark Module").

4.1. Support. Customer will receive email support for the Benchmark Module by emailing unmetric-help@brandwatch.com and will receive a response within 24 hours. Supplier will use commercially reasonable efforts to: (a) fix bugs within a reasonable time; and (b) make the Benchmark Module available 24 hours a day, 7 days a week, except for: (i) planned downtime (of which Customer will receive notice by email at least 6 hours in advance); or (ii) any unavailability caused by circumstances beyond Supplier's reasonable control.

5. Professional Services terms

This section 5 only applies if Customer's Order includes any custom professional services that Supplier provides to Customer ("Professional Services").

5.1. Deliverables. Supplier owns any Deliverable, excluding any Customer Data in a Deliverable. Supplier grants to Customer a worldwide, non-exclusive, non-transferable, royalty-free licence to use the Deliverable and the Supplier Data in the Deliverable in accordance with this Agreement.

5.2. Hours. Supplier will provide Customer with Professional Services for the number of hours set out on an Order ("Hours"). Any time allocated by Supplier to provide Professional Services to Customer (including

preparatory work) will be deducted from Customer's allotted Hours. Use of Hours will be coordinated with Customer upon Customer's request. Supplier may charge Customer additional fees for training if Customer repeatedly fails to attend its training session(s) or cancels with less than 24 hours' notice. Unused Hours are not usable or reimbursable upon expiration or termination of an Order.

5.3. Delays. Customer will promptly provide Supplier with any data as requested by Supplier to deliver the Deliverables. Customer is not entitled to a reimbursement of fees in the event of delays or incomplete Deliverables caused by Customer's non-fulfilment of its obligations under this Appendix.

6. Agency Terms

This section 6 only applies if Customer is subscribed to the Services or Benchmark Module or Professional Services as an agency to render its own agency services to its clients ("Agency Clients"). Customer shall abide by the terms available at <https://www.cision.com/legal/service-appendices/agency-service-appendix/>.

7. API terms

This Section 7 only applies if Customer's Order includes the API or API+ products.

7.1. "API Documentation" means Supplier's documentation set out in the [Help Center](#) or as otherwise provided by Supplier.

7.2. Licence. Supplier grants to Customer a non-exclusive, revocable, non-transferable, non-sublicensable licence to access and use the API in accordance with this Appendix for the purposes of exchanging data between the Services and Customer's system, subject to a use case approval granted by Supplier ("API Licence"). Unless otherwise agreed, Customer is granted up to five API keys for use within a single legal entity ("Organisation") and such API keys may only be shared within such Organisation. Notwithstanding the previous sentence, Customer is entitled to share the API key with one of Customer's authorised third parties provided that the API key is used for Customer's internal use. Any API integration developed by Customer, or by a third party on Customer's behalf, will comply with the terms of this Agreement. When accessing content via an API, Customer agrees to refresh all API queries at least daily, or more frequently upon request of Supplier.

7.3. Miscellaneous. For the purposes of this Appendix, the API is part of the Services and all rights, restrictions and obligations (including disclaimers and exclusions of liability) with respect to the Services apply to the API. Notwithstanding the previous sentence, Supplier may terminate the API Licence for convenience at any time and, provided that Customer is not in breach, Supplier will provide a pro-rata refund of any prepaid fees for the API Licence. Supplier reserves the right to validate Customer's use of Supplier Data obtained via API and Customer agrees to comply with Supplier's reasonable requests. In the event of any conflict among the documents identified in these API terms, the order of precedence will be: (a) the API Documentation; (b) these API terms; (c) Section 2 of this Appendix; and (d) the Master Agreement.

7.4 Restrictions. Unless Customer obtains express written consent from Supplier or Customer is otherwise permitted in its direct agreements with relevant third-party content providers, Customers who leverage the API and API+ products are prohibited from using Supplier Data in the following ways:

- Advertising or earning advertising revenue of any type in any downstream product in connection with the use of any IP contained in the API,
- Using the data or any data derived therefrom, or permitting users of each downstream product, to use such data in any manner that competes with Supplier or any data providers whose information is contained in the API,
- Using the data in the API to create a historical database,
- Any use in connection with generative AI or large language models, including the training of such programs,
- Make available, share with, sell to, or syndicate with any third parties, including for use in any litigation, arbitration mediation, or other legal, regulatory, administrative, or similar proceeding,
- To investigate, track, or survey users whose PII may be included in the API and/or their content, or to obtain any information regarding users or their content in any manner that would require a court order, subpoena, or other judicial or governmental directive,
- To use, or knowingly display, distribute, or otherwise make data within the API available to any government end user for conducting surveillance, gathering intelligence, or law enforcement purposes,
- To track, alert, or monitor sensitive events (such as protests, rallies, or community organizing meetings) for surveillance or other unlawful purposes, including tracking individuals who are part of such sensitive events; to investigate or track sensitive groups or organizations such as unions or activist groups for surveillance or other unlawful purposes; to perform background checks or any form of extreme vetting; to perform credit or risk insurance analyses, individual profiling, or psychographic segmentation; or to perform facial recognition, or
- To derive or obtain non-public information of individuals whose PII may be included in the API, including without limitation, a user's location, household, device, browser, individual, or other identifier.

8. Third-party services

Each subsection in this Section 8 only applies if Customer's Order includes the relevant third-party services.

- 8.1 Trajaan. Customer will comply with the Trajaan terms and conditions usually at <https://trajaan.io/terms-conditions/>.