

Media Database Service Appendix – last updated: 3 October 2025

This Media Database Service Appendix (“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

For the purposes of this Appendix, references to “Services” in the Master Agreement refer to the Platform (defined below).

“**Platform**” means the on-demand relationship management and communications technology and services that Supplier provides to Customer.

“**Supplier Data**” has the meaning set out in the Master Agreement, and in the context of the “media database” or “outreach” module consists of names, email addresses, phone numbers, social handles, and other general details for journalists, influencers and other noteworthy individuals.

2. Service terms

2.1. License. Supplier grants to Customer a non-exclusive, revocable, non-transferable, non-sublicensable license to use the Supplier Data during the Term to create and download lists of media outlet data, distribute communications via the Platform, and attach its notes to Supplier Data. Users may integrate their email account into the Platform to view email correspondences sent outside the Platform with contacts found in the Supplier Data. If a User authorizes such integration, Supplier or its third-party service providers will search, index and copy email messages from an integrated email account, and store and display those email messages within the Platform for Customer’s use.

2.2. Restrictions. Customer will not: (a) remove any proprietary notices, graphics or text contained in the Supplier Data; (b) make the Supplier Data available to non-Users; or (c) incorporate or use the Supplier Data in any resale process, including a press release distribution service; or (d) use the 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.

2.3 Privacy notices. 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.

2.4. Responsibility. Customer will comply with the X, formerly Twitter, Terms of Service, usually at <https://twitter.com/tos>, and 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>, 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. Further, 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. From the point of download, Customer will be responsible for all Supplier Data that it downloads from the Services, including responsibility for data protection and data processing regulations.

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 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 US intelligence community or any other government or public-sector entity.

2.6. Removal of Supplier Data. Under Applicable Law a data subject may require Supplier to remove personal data from Supplier Data. If Supplier is aware that Customer has downloaded such personal data, Supplier will use reasonable efforts to notify Customer of the impacted Supplier Data that requires removal and Customer will promptly remove such data from its systems.

2.7. Availability. The Platform will maintain an average availability of no less than 99.5%, as measured on a monthly basis, excluding downtime caused by (1) scheduled maintenance performed between the hours of 12:00 AM and 6:00 AM Eastern time; (2) emergency maintenance; and (3) force majeure. Access to the Platform may be available during scheduled maintenance periods, but performance may be slower than normal.

2.8. Support. Customer will have unlimited access to Supplier's online product support center.

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

2.10. Customer Data Availability. 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. Disclaimers. Supplier does not maintain or control and is not responsible for third-party content or the links to other websites that may be made available via the Services or within Reports, which are, at all times, subject to the terms and policies of the third-party content provider. Supplier Data is provided "as is", exclusive of any express or implied warranties. 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 ceases to make its content, features, or functionality available, Supplier disclaims all liability for the unavailability of such content, features, and functionality.

2.12. 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. Agency Terms

This section 3 only applies if Customer is an agency, using the Services on behalf of its own clients ("Agency Clients"). Customer shall abide by the terms available at <https://www.cision.com/legal/service-appendices/agency-service-appendix/>.

4. API Terms

This Section 4 only applies if Customer's Order includes an API.

4.1. License. Subject to Customer's use case being approved, Supplier grants to Customer a non-exclusive, revocable, non-transferable, non-sublicensable license to access and use the API in accordance with this Appendix for the purposes of exchanging data between the Services and Customer's system ("API License"). Unless otherwise agreed, Customer is granted up to five API keys for use within a single legal entity ("Organization") and such API keys may only be shared within such Organization. Notwithstanding the previous sentence, Customer is entitled to share the API key with one of Customer's authorized 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.

4.2. 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 License 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 License. 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.

4.3 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 Supplier's API 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.