

PRIVACY ADDENDUM TO THE TERMS OF SERVICE FOR THE ACCESS AND USE OF THE TALKWALKER PLATFORM AND SERVICES, AS OF JUNE 10, 2020 (“ADDENDUM”)

1. SUBJECT MATTER, PARTIES AND DEFINITIONS

- 1.1. This Addendum. This Addendum governs the privacy and data protection framework for processing activities on the Covered Data (as defined below), performed as a result of the access and use of the Talkwalker Platform and Services, and as further defined in Appendix 1.
- 1.2. Service Provider. The Talkwalker Platform and Services are subject to and provided in compliance with applicable Privacy Laws (as defined below). For the purpose of this Addendum, Talkwalker acts as a processor, or in an equivalent role, under applicable Privacy Laws.
- 1.3. Client. All processing activities on the Talkwalker Platform are performed by Talkwalker on the documented instructions of the business or Client. For the purpose of this Addendum, Client acts as a controller and determines the purposes and means of the processing of Covered Data.
- 1.4. Instructions. Talkwalker carries out processing activities only once instructed by the Client under either (i) an Order Form, (ii) other written instruction, including those relating to the essential means of processing, or (iii) specific search, set up, or configuration of the Talkwalker Platform, to process Covered Data.
- 1.5. Definitions. All capitalized terms not defined herein shall have the meaning as set forth in the Contract. The below terms shall have the following meanings:
 - 1.5.1. “Breach” means any compromise of security measures that leads to an accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Covered Data;
 - 1.5.2. “Contract” means an agreement, including this Addendum, under which Talkwalker provides access to Talkwalker Platform or renders the Services;
 - 1.5.3. “Covered Data” means personal information and data collected and processed by Talkwalker on behalf of the Client within the framework or as a result of of the access and use of Talkwalker Platform and Services by the Client and as further defined in Appendix 1;
 - 1.5.4. “Data Transfer” means transferring Covered Data outside of the European Economic Area by Talkwalker on request of the Client;
 - 1.5.5. “Privacy Laws” means all applicable laws and regulations relating to privacy and data protection, to which Talkwalker is subject as service provider of the Talkwalker Platform and processor of the Covered Data.

2. CLIENT’S RIGHTS AND OBLIGATIONS

- 2.1. Purpose, nature, and means of processing. The purpose, nature, and means of processing are described in Appendix 1. In regards to the purpose of data processing, the Client understands and warrants that it shall not use or process, or request Talkwalker to process, the Covered Data in any manner which violates Privacy Laws and that it will use all required procedures and safeguards.
- 2.2. Assistance. Talkwalker shall use reasonable efforts to assist the Client to comply with the latter’s duties relating to privacy or data protection impact assessments. Talkwalker shall

provide all reasonably required information and documents to the Client in order to prove compliance with its obligations under this Addendum.

- 2.3. Audit rights. Talkwalker may provide assistance to the Client should the Client wish to conduct an audit of the data processing undertaken by Talkwalker on behalf of the Client.
- 2.4. Costs. Reasonable costs relating to the assistance and audit, or any other services rendered by Talkwalker to the Client, may be charged if they unduly interfere with the normal operations of Talkwalker's business, in particular if the Client provides a written notice shorter than two (2) weeks, or if the audit lasts more than one (1) day during every twelve (12) month period. In any case, the Client shall bear the costs of any external auditor, and any costs related to the audit of sub-processors.
- 2.5. Findings. The findings of the audit shall be evaluated and discussed by the parties. Any resulting additional measures agreed upon by the parties shall be implemented by the relevant party without undue delay.
- 2.6. Supervisory authorities. To the extent permitted, the Client undertakes to inform Talkwalker without undue delay of any audits, inspections, or other measures taken by a competent supervisory authority in relation to the processing of Covered Data. The parties shall collaborate in good faith in responding to such enquiries.

3. PROCESSOR

- 3.1. Talkwalker. Talkwalker must not sell, retain, use, or disclose the Covered Data for any purpose any other than for the specific purpose of performing the services specified in the Contract and as further defined in Appendix 1. Further, Talkwalker understands and will comply with all of its contractual restrictions related to the processing of Covered Data.
- 3.2. Compliance. Notwithstanding Client's ongoing duty to ensure the lawfulness of processing, Talkwalker shall use its commercially reasonable efforts to inform the Client if the latter's instructions may be deemed to violate applicable Privacy Laws, including considering the information made available by the Client. If the instructions of the Client are deemed unlawful by Talkwalker, the latter is entitled to suspend the execution of such instructions until the lawfulness of such instructions is verified and confirmed in writing by the Client and, at the request of Talkwalker, by outside counsel of the Client.
- 3.3. Security. Taking into account the state of the art, the costs of implementation, the nature and risks of the processing activities relating to the Covered Data as well as appropriate industry standards, Talkwalker undertakes to use its commercially reasonable efforts to implement appropriate technical and organisational measures in order to safeguard the protection of Covered Data. The parties agree to implementation of the technical and organisational measures as set out in Appendix 2.
- 3.4. Amendments. During the course of the Addendum, the Client may request Talkwalker to offer the implementation of additional technical or organisational measures. In such case, Talkwalker shall inform the Client, at its discretion, if such additional measures are feasible from a technical and organisational standpoint and, if it deems such measures feasible, Talkwalker shall inform the Client of the costs involved with the implementation of such measures. If the offer is accepted by the Client, Talkwalker shall implement the additional measures in accordance with the conditions agreed upon by the parties.

3.5. Requests. If a data subject addresses a verifiable request to the Client regarding processing performed by Talkwalker under the scope of this Addendum, the Client shall redirect such request to Talkwalker within a reasonable timeframe which must not exceed seven (7) business days. Talkwalker shall use its commercially reasonable efforts to comply with such request within a reasonable timeframe.

4. SUB-PROCESSING

4.1. Authorisation. Talkwalker is authorised to engage sub-processors for processing operations in the provision of the Services, without the prior specific approval of the Client being required so long as the new sub-processor provides a level of protection for the Covered Data materially similar to the level of protection previously provided. The Client acknowledges the sub-processors listed in Appendix 1 process Covered Data in the provision of the Services and agrees to such appointment by entering into this Addendum.

4.2. Sub-processors. Talkwalker undertakes to impose on any sub-processor, by means of a contractually binding agreement, data protection obligations which are materially similar to those set out in this Addendum. Talkwalker remains liable for the sub-processor's failure of its obligations, subject to the limitation of liability under the Contract.

4.3. Clarification. The parties agree that the term "sub-processor" does not refer to contractual service providers which provide ancillary services and which Talkwalker may have recourse to in the provision of the Services under the Contract, including telecommunication services, postal services, and office maintenance services.

4.4. Details. In case of engagement or replacement of a sub-processor, Talkwalker shall need only to inform the Client in writing prior to any appointment or replacement of a sub-processor. This prior information notice shall contain a description of the nature of the processing activities concerned as well as the designation of the sub-processor.

4.5. Right to object. If the Client objects, within thirty (30) calendar days of receipt of the notice of information, to the use of the sub-processor concerned, Talkwalker shall have the right to cure the objection through one of the following options: (i) not to use the sub-processor with regard to the Covered Data; (ii) to take the corrective steps requested by the Client (which remove Client's objection) and proceed to use the sub-processor with regard to Covered Data; or (iii) to cease to provide or the Client may agree not to use (temporarily or permanently) the particular aspect of the Service that would involve use of the sub-processor.

5. TRANSFER OF COVERED DATA

5.1. Data Transfer. All processing activities take place and Covered Data are hosted on data centres located in the European Union. Talkwalker may only transfer any Covered Data outside of the European Union when instructed to do so by the Client or in the event of a data transfer to an authorised sub-processor.

5.2. Safeguards. Any transfer of the Covered Data must comply with the applicable Privacy Laws, in particular by putting in place adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals and the exercise thereof, in particular by execution of applicable standard contractual clauses for the transfer of personal data adopted by the European Commission or other relevant supervisory authority.

6. COVERED DATA BREACH

- 6.1. Breach. Talkwalker undertakes to notify the Client of a Breach without undue delay, and if possible, within twenty-four (24) hours, after becoming aware of such Breach. The content of the notification shall fulfil no less than the minimum requirements of the applicable Privacy Laws.
- 6.2. Information. Where, and in so far as, it is not possible for Talkwalker to provide the information at the same time, the information shall be provided to the Client in phases without undue further delay.
- 6.3. Notification. The Client undertakes to notify a competent supervisory authority of the Breach without undue delay and, if applicable, to the data subjects concerned if such notification is required under applicable Privacy Laws. The Client shall inform Talkwalker prior to any such notification taking place in order to allow, to the maximum extent possible, to take into account the observations presented by Talkwalker in relation to the proposed draft of the notification.
- 6.4. Support. Upon request and written instruction of the Client, Talkwalker may accept to handle, on behalf of the Client, the notification of a Breach to a competent supervisory authority and/or to the data subjects concerned, as the case may be.

7. REPRESENTATIONS AND WARRANTIES, LIABILITY

- 7.1. Liability. Each party's liability arising out of or related to this Addendum, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability section as agreed upon in the Contract and any reference in such section to the liability of a party means the aggregate liability of that party and all of its affiliates under the Contract and all data processor agreements taken together.
- 7.2. Warranties. Talkwalker will use its commercially reasonable efforts to ensure an appropriate level of protection of personal data, in particular by maintaining the technical and organisation measures described in Appendix 2.
- 7.3. Exclusion. The Client is responsible for ensuring that the data processing which it instructs Talkwalker to undertake is lawful and pursues legitimate and proportionate purposes. Moreover, Talkwalker shall not be liable for the processing of Covered Data undertaken by the Client itself or by third parties acting under Client's instructions.

8. MISCELLANEOUS

- 8.1. Duration. This Addendum may be terminated or expire only in connection with the terms of the Contract.
- 8.2. Deletion. After the provision of the Services related to Covered Data have terminated, the parties agree that the Covered Data shall be deleted as soon as is reasonably possible. Upon Client's request, a written confirmation will be provided. Upon separate written agreement, and in any case prior the expiry or termination date of the Contract, the Client may request a copy of Covered Data against payment of the reasonable costs incurred by Talkwalker to render such service.
- 8.3. Legal retention. Notwithstanding the foregoing, Talkwalker shall be entitled to retain a copy of Covered Data as long as required for evidentiary or statutory record retention purposes.
- 8.4. Confidentiality. Talkwalker confirms that all personnel who are involved in the processing activities are subject to a duty of confidentiality.

- 8.5. Entire Agreement. This Addendum together with its appendices supersedes any and all other prior or contemporaneous understandings and agreements, either oral or in writing, between the parties with respect to the subject matter hereof and constitutes the sole and only agreement between them with respect to its subject matter.
- 8.6. Amendments. This Addendum may be amended only by a written instrument which specifically refers to this Addendum. Unless otherwise agreed in the Contract, Talkwalker shall be entitled to amend this Addendum by providing thirty (30) calendar days prior written notice to the Client.
- 8.7. Notices. Each party shall give all notices to the other party in writing, including by e-mail.
- 8.8. Governing law and place of jurisdiction. This Addendum shall be governed by the laws governing the Contract, without giving effect to conflicts of law principles. Any action, proceeding or claim arising out of or relating in any way to this Addendum shall be brought and enforced in the courts which have jurisdiction over the Contract.

APPENDIX 1. DETAILS OF THE PROCESSING ACTIVITIES

1. Subject matter and purposes. The processing activities of the Covered Data shall involve carrying out web and social media listening and analytics for brand monitoring purposes.
2. Nature. The nature of the processing activities consists of collecting, sorting, saving, transferring, restricting, and deleting of Covered Data in the context of Client's use of the Talkwalker Platform and Services.
3. Means. The Client shall have the following means of processing activities:
 - 3.1. Covered Data to be collected and further processed in relation to the specific searches in the Talkwalker Platform;
 - 3.2. the web, social media, and other media types to be searched;
 - 3.3. the identity of persons authorised to access Covered Data in the Talkwalker Platform;
 - 3.4. the access rights of such users of the Talkwalker Platform;
 - 3.5. the retention period of Covered Data.
4. Data subjects. The categories of data subjects are customers and potential customers (consumers) of the Client.
5. Covered Data. The following types of Covered Data are collected, processed, and/or used within the Talkwalker Platform:
 - 5.1. identification data defined as unique identifiers associated with social media and web users ("Authors"), such as name, username, user ID, geolocation data, or similar;
 - 5.2. socio-biographical data defined as publicly available personal characteristics of Authors, such as age, gender, consumer habits, hobbies, interests, ambition, professional and educational background, as well as photos and videos;
 - 5.3. Authors' content defined as a specific status update or comment, or item on a blog or forum that contains keywords and characteristics, and any other brand monitoring related information published by the Authors' on a publicly available Internet website or on a third-party platform that fits the search criteria when associated with any identification data and/or socio-biographical data relating to Authors.
6. Duration. The duration of the processing activities under this Addendum corresponds to the duration of the Contract.
7. Data Protection Officer. The data protection officer can be reach via dpo@talkwalker.com.
8. Sub-processors. The list of sub-processors relevant for the processing activities on the Talkwalker Platform:
 - 8.1. hosting provider: Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Germany, Data Protection Officer can be reached via data-protection@hetzner.com.

APPENDIX 2. TECHNICAL AND ORGANISATIONAL MEASURES

1. Confidentiality. Talkwalker's employees are subject to background checks and are bound by confidentiality obligations subject to their employment agreement and applicable law. Further measures include:
 - 1.1. physical access controls:
 - 1.1.1. electronic physical entry control system with log;
 - 1.1.2. visitors need to be escorted by an employee or bound by non-disclosure agreements;
 - 1.1.3. fire and intrusion alarms;
 - 1.2. regularly reviewed electronic access controls regarding production server administration:
 - 1.2.1. dedicated servers fully managed by Talkwalker (no hypervisor or virtualization);
 - 1.2.2. MFA for production server administration;
 - 1.2.3. computers accessing the production are connected to a separate network;
 - 1.3. regularly reviewed electronic access controls via the platform:
 - 1.3.1. logical segregation of data between clients;
 - 1.3.2. the Client (as an account admin) manages its users and detailed access rights;
 - 1.3.3. access to Covered Data by Talkwalker on a need-to-know basis (e.g. sales representatives, account managers, finance department);
 - 1.3.4. Talkwalker employees log into the platform using an internal Single Sign-On (SSO) using 2-factor authentication, the Clients can also link the access to their internal SSO (e.g. Active Directory) using SAML 2.0;
 - 1.4. management of media regarding datacentres:
 - 1.4.1. full disk encryption using AES-128 algorithms for all production servers hosting non-public data;
 - 1.4.2. drives that were in operation on cancelled servers are wiped multiple times (deleted) by hosting provider in accordance with data protection polices;
 - 1.4.3. defective drives that cannot be securely deleted shall be destroyed (shredded) directly in the datacentre;
 - 1.5. management of media regarding workstations:
 - 1.5.1. full disk encryption using AES-128 algorithms for mobile workstations used by Talkwalker employees.
2. Integrity. The integrity of Covered Data is assured by the following measures:
 - 2.1. data transfer controls:
 - 2.1.1. clients access the Talkwalker platform using state of the art HTTPS/TLS;
 - 2.1.2. all Talkwalker employees receive training on privacy and security matters;
 - 2.1.3. deletion of Covered Data in accordance with Privacy Laws;
 - 2.2. data input controls:
 - 2.2.1. Covered Data is entered, collected, and can be visualised on the Talkwalker Platform;
 - 2.2.2. changes in Covered Data by the Client and Talkwalker employees are logged in a separate dedicated audit log system; logs can be provided to the clients;
 - 2.3. secure infrastructure and development:
 - 2.3.1. internal development guidelines, developer talks, regular training of developers and engineers;
 - 2.3.2. passwords are salted and hashed (i.e. plain-text passwords are not retained);

- 2.3.3. network segregations at both the datacentre (production vs test) and office (wireless vs development vs access to production).
- 3. Availability, reliability, and resilience. Further security measures include:
 - 3.1. measures relating to the hosting provider:
 - 3.1.1. processing and hosting of Covered Data take place in dedicated infrastructures, holding a valid ISO 27001:2013 certificate;
 - 3.2. availability controls:
 - 3.2.1. backup and recovery concept with daily backups of all Covered Data to a datacentre located in a remote location;
 - 3.2.2. replication of services to account for the most common hardware failures;
 - 3.2.3. 24-hours monitoring and alerting of all servers and services;
 - 3.2.4. employment of UPS or emergency power supply systems;
 - 3.2.5. rapid provisioning of servers to accommodate scaling demand of resources;
 - 3.3. protection against threats:
 - 3.3.1. professional employment of security programs, including both network-based and host-based firewalls, as well as DDoS protection;
 - 3.3.2. network and server configurations are security-hardened;
 - 3.3.3. virus and malware protection by default with daily updates of definitions and signatures;
 - 3.3.4. monthly security patch deployment on critical assets.
 - 3.4. rapid recovery measures:
 - 3.4.1. there is a defined escalation chain which specifies who is to be informed in the event of an incident in order to restore the system as quickly as possible;
 - 3.4.2. Talkwalker has business continuity and disaster recovery procedures to accelerate and standardise recovery works;
- 4. Continuous improvement. In order to maintain the state of the art technical and organisational measures, Talkwalker regularly tests, assesses, and evaluates the implemented measures and the related risks, in particular by:
 - 4.1.1. having dedicated employees in order to implement and apply an information security management system aligned with the international standard ISO27001:2013;
 - 4.1.2. having an incident management procedure in place covering security, privacy and data protection topics that may arise and include escalation procedures in case notifications to data subjects, clients, or supervisory authorities are required;
 - 4.1.3. regularly mandating an independent organisation to perform intrusion tests on the Talkwalker Platform;
 - 4.1.4. having written agreements with its sub-processors in order to ensure that Talkwalker obligations are replicated to them in accordance with this Addendum; before engaging a new sub-processor, Talkwalker carries out security and data protection risk assessment, which are proportionate to the sensitivity of the Covered Data handled by the sub-processor, except in the events where the sub-processor owns an independent security certification on which Talkwalker can rely.