Data Processor Agreement or "DPA"
Version May 18th 2018

INTRODUCTION

For its Services, Talkwalker crawls websites including social and web media platforms. In this context Talkwalker decides what data it collects and how and why this data is used in connection with the Talkwalker Platform. Our data collection and processing are not specific to any particular customer and is therefore not considered as being processed on the instructions of any customer.

Consequently for the data it processes independently of any customer instruction, Talkwalker considers itself:

- a *data controller* under the GDPR for personal data contained on its platform
- and undertakes that the features of the platform are compliant with GDPR principles.

For personal data input by customer or specific requests made by customer on the platform, Talkwalker technically acts as *data processor* for the customer as it follows the instructions of the customer to input and process the data, of which some may be personal data.
As a data processor, Talkwalker commits to ensuring that appropriate technical and organizational security measures as required under the GDPR. Those measures are in place to protect customer data as set out in the below data processor agreement between Customer and Talkwalker.

DATA PROCESSOR AGREEMENT

Controller and Processor have entered into a main agreement ("Main Services Agreement") regarding the provision of brand monitoring services ("Services") by Processor to Controller.

Controller is the Customer of Talkwalker, including Customer's Affiliates where relevant, as set out in the Main Services Agreement. Processor is the Talkwalker entity contracting with Customer in the Main Services Agreement.

In order to provide the Services under the Main Services Agreement, Controller requires Processor to process, on its behalf, the personal data provided or input by customer or specific requests made by customer on the platform ("Customer Personal Data").

Controller has elected to appoint Processor to provide the Services and has determined the purposes and the essential means of the data processing to be carried out by Processor on behalf of Controller.

The Parties have decided to enter into this DPA, effective as of 25 May 2018, to set out their rights and obligations in relation to the processing of Personal Data by Processor in accordance with Article 28 of Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data (hereinafter the "GDPR").

ARTICLE 1 – SUBJECT MATTER OF THE DPA AND DEFINITIONS

1.1. This DPA defines the respective rights and obligations of each Party in relation to the processing of Personal Data carried out by Processor on behalf of Controller.

1.2. Except as otherwise expressly provided or unless the context otherwise requires, the terms used in this DPA shall have the meaning attributed to them in the GDPR, in this DPA as well as in the Main Services Agreement.

ARTICLE 2 – DESCRIPTION OF THE DATA PROCESSING UNDERTAKEN BY PROCESSOR

2.1. Processor is instructed by Controller to process Customer Personal Data within the framework of the Services provided by Processor under the Main Services Agreement.

The categories of Personal Data and of data subjects concerned by the data processing are set out in Attachment 1.

2.2. Processor shall process the Personal Data only in accordance with the instructions of Controller. The instructions are provided within the framework of the Main Services Agreement between the parties.

2.3. Controller undertakes to confirm, in writing, all instructions given to Processor in relation to the processing of Personal Data, by the following means:

- the order form for the Services,
- the written instructions given to the Support or Customer Success Manager (CSM) team,
- the confirmation of the Use Case by Controller through the execution of an order form or any equivalent contractual document, including by exchange of e-mails,
- the set up and configuration of the Talkwalker Platform, and
- the specific searches made by Controller in the Talkwalker Platform.

2.4. Processor undertakes to process Personal Data only as instructed by Controller through the provision of the Services.

ARTICLE 3 – DUTIES OF THE PARTIES

3.1. Controller has determined the purpose(s) of the data processing before engaging the Services of Processor. The nature of the data processing and the purpose(s) of the data processing are described in Attachment 1.

3.2. Controller has also defined the essential means of data processing, including:

- the Personal Data to be collected in relation to the specific searches of the Customer,
- the categories of Personal Data to be processed on its behalf by determining the social media channels and other media types to be searched,
- the identity of persons authorized to access Personal Data in the Talkwalker Platform, the access rights of such users of the Talkwalker Platform, and
- the retention period of Personal Data.

The essential means of data processing as determined by Controller may be modified at any time by addressing a request, in writing, to the Support team or the Customer Success Manager (CSM) team of Processor or by changing the appropriate settings in the Talkwalker Platform.

3.3. In regards to the purpose(s) of data processing, Controller represents and warrants that it shall not use or process, or request Processor to process, the Personal Data in any manner which infringes upon the rules laid out in the GDPR or in any other applicable law and that it will use relevant procedures and safeguards as required to protect such Personal Data.

3.4. Without prejudice to Controller's duties to ensure the lawfulness of data processing, Processor shall use its best commercially reasonable efforts to inform Controller if the latter's instructions may be deemed to infringe upon the provisions of the GDPR, including but not limited to taking into account the information made available by Controller. If the instructions of Controller are deemed unlawful by Processor, the latter is entitled to suspend the execution of such instructions until the lawfulness of such instructions is verified and confirmed in writing by Controller and, at the request of Processor, by outside counsel of Controller.

3.5. Taking into account the state of the art, the costs of implementation, the nature and the risks of Personal Data processing as well as appropriate industry standards, Processor undertakes to use its best commercially reasonable efforts to implement appropriate technical and organizational measures in order to safeguard the protection of Personal Data and the processing of such Personal Data. The Parties agree to the implementation by Processor of the technical and organizational measures set out in Attachment 2.

3.6. During the course of the DPA, Controller may request Processor to make an offer for the implementation of additional technical or organizational measures. In such case, Processor shall inform Controller, at its discretion, if such additional measures are feasible from a technical and organizational standpoint and, if it deems such measures feasible, Processor shall inform Controller of the costs involved with the implementation of such measures. If the offer is accepted by Controller, Processor shall implement the additional measures in accordance with the conditions agreed upon by the Parties.

3.7. In order to safeguard the protection of Personal Data and the processing of such Personal Data to the best of its ability, by taking into account technical progress and recognized state-of-the-art developments implemented in Processor's industry, Processor may decide - at its discretion - to adapt and amend Attachment 2 in order to implement additional technical or organizational measures in the course of performance of the DPA or to modify the technical and organizational measures implemented at the date of entering into force of this DPA or at a later stage. In such case, Processor undertakes to maintain an appropriate level of protection of Personal Data and of the processing of such data. Substantial changes to the technical and organizational measures implemented by Processor shall be documented and communicated to Controller in accordance with Article 12.2 of this DPA.

3.8. Processor undertakes to monitor the adequacy of the protection of the technical and organizational measures at regular intervals.

3.9. Processor undertakes to process Personal Data as instructed by Controller, except if Processor is required to do so by law or in the context of a potential dispute concerning, for instance, the delivery of the Services to Controller.

ARTICLE 4 – RIGHTS OF THE DATA SUBJECTS

4.1. If a data subject addresses a request to Controller regarding data processing performed by Processor under the scope of this DPA, Controller shall redirect such request to Processor within a reasonable timeframe which must not exceed seven (7) business days. Processor shall use its best commercially reasonable efforts to comply with such request within a reasonable timeframe.

ARTICLE 5 – PERSONAL DATA BREACH

5.1. Processor undertakes to notify Controller of a Personal Data breach compromising Controller's Personal Data without undue delay, and if possible within twenty-four (24) hours, after becoming aware of said breach.

5.2. In the context of the Personal Data breach notification to Controller, Processor shall provide the following information:

- description of the nature of the Personal Data breach including, where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of Personal Data records concerned;
- description of the likely consequences of the Personal Data breach;
- description of measures taken or proposed to be taken in order to address the Personal Data breach, including, where appropriate, measures to mitigate its possible adverse effects;
- the contact details of the Data Protection Officer or other contact person who can provide any additional information required.

Where, and in so far as, it is not possible for Processor to provide the information at the same time, the information shall be provided to Controller in phases without undue further delay.

5.3. Controller undertakes to notify the competent data protection supervisory authority of the Personal Data breach without undue delay and, if applicable, to the data subjects concerned if such notification is required under the GDPR or any other applicable legislation. Controller shall inform Processor prior to any such notification taking place. Controller shall, to the maximum extent possible, take into account the observations presented by Processor in relation to the proposed draft of the Personal Data breach notification.

5.4. Upon request and written instruction of Controller, Processor may accept to handle, on behalf of Controller, the notification of a Personal Data breach to the competent data protection supervisory authority and to the data subjects concerned, as the case may be.

ARTICLE 6 – ASSISTANCE AND AUDIT

6.1. Processor shall use reasonable efforts to assist Controller to comply with the latter's duties in regards to data protection impact assessments required under the GDPR and/or by any competent

authority and any related prior consultation processes with the relevant data protection supervisory authority.

6.2. Processor shall provide all reasonably required information and documents to Controller in order to prove compliance with its duties under this DPA. In this context and in order to confirm compliance, Controller shall be entitled to conduct an audit of the data processing undertaken by Processor on behalf of Controller.

Controller and Processor shall agree in writing on the reasonable conditions under which such audit may be carried out. In any case, any audit will have to comply with Processor's reasonable requirements, such as in terms of security, confidentiality, and the protection of intellectual property rights and business secrets. In particular, if the audit is carried out by a third party on behalf of Controller, such third party may not be a competitor of Processor and must sign a non-disclosure and confidentiality agreement, without prejudice to other conditions that may reasonably be imposed by Processor.

Any audit may not unduly interfere with the normal conduct of Processor's business. Controller will, in principle, provide at least two weeks' prior written notice of an audit request.

The findings of the audit will be evaluated and discussed by the Parties. As the case may be, the resulting additional measures agreed upon by the Parties shall be implemented by the relevant Party as soon as reasonably possible.

6.3. To the extent required and if Controller does not have direct access to the relevant information, Processor shall also endeavor to assist Controller to comply with the latter's duty to respond to legitimate requests of data subjects relating to their rights under the GDPR.

6.4. Reasonable costs relating to the audit and any other services rendered by Processor to assist Controller may be charged by Processor to Controller. Controller shall bear the costs of any external auditor appointed by it to perform an audit.

6.5. To the extent permitted, Controller may also request Processor to audit a Sub-Processor by complying with such Sub-Processor's reasonable requirements. Controller shall bear any reasonable costs charged by Processor and such Sub-Processor regarding such audit.

6.6. To the extent permitted, Controller undertakes to inform Processor without undue delay of any audits, inspections, or other measures taken by the data protection supervisory authority or by any other competent authority in relation to the processing of Personal Data relating to this DPA. Such notification shall be made free of charge and shall contain the essential elements describing the subject matter of the relevant authority's action. The Parties shall cooperate in good faith in responding to such enquiries.

ARTICLE 7 - TRANSFERS OF PERSONAL DATA OUTSIDE OF THE EU

7.1. Processor shall not transfer any Personal Data outside of the European Union ("EU"), unless instructed to do so by Controller or unless Personal Data is transferred to Sub-Processors approved by Controller in accordance with Article 9 of this DPA.

7.2. If Controller instructs Processor to export Personal Data outside of the EU, it shall ensure that such export complies with the conditions set out in the GDPR and in any other applicable data protection legislation and the Standard Export Terms as provided as Attachment 4 shall apply.

7.3. If Processor is required to transfer Personal Data outside of the EU by virtue of law, by virtue of the order of a court or of any other competent authority, Processor shall endeavor to inform Controller prior to such transfer, except if such information is prohibited by law.

ARTICLE 8 – REPRESENTATIONS AND WARRANTIES, LIABILITY

8.1. Each Party's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the limitation of liability section as agreed upon in the Main Services Agreement 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 Main Services Agreement and all data processor agreements taken together.

8.2 Processor shall be solely responsible to use its best commercially reasonable efforts for the processing of Personal Data in accordance with this DPA. Even though Processor cannot guarantee that the technical and organizational security measures shall be effective under all circumstances, Processor will use its best commercially reasonable efforts to ensure that the level of protection of Personal Data and of the processing of Personal Data is appropriate, as set out in Article 3 of this DPA.

8.3. Controller is responsible for ensuring that the data processing it instructs Processor to undertake is lawful and that it pursues legitimate and proportionate purposes. Moreover, Processor shall not be liable for the processing of Personal Data undertaken by Controller itself or by third parties acting under Controller's instructions.

ARTICLE 9 – SUBPROCESSING

9.1. As permitted by Article 28 3° of the GDPR, Controller hereby generally authorizes Processor to engage sub-processors for specific data processing operations ("Sub-Processor(s)") as deemed appropriate by Processor in the provision of the Services, without the prior specific approval of Controller being required to the extent the new Sub-Processor provides a level of protection for the Personal Data processing that is materially similar to the level of protection previously provided.

9.2. In case of engagement or replacement of a Sub-Processor, Processor shall need only to inform Controller in writing prior to any envisaged appointment or replacement of a Sub-Processor. This prior information notice shall contain a description of the nature of the Personal Data processing activities concerned as well as the designation of the Sub-Processor. Controller shall be entitled to formulate written objections to the appointment or replacement of a Sub-Processor within thirty (30) days of the receipt of the notice of information if it has a legitimate, material reason to object. If Controller objects to the use of the Sub-processor concerned, Processor shall have the right to cure the objection through one of the following options: (i) Processor will abort its plans to use the Sub-processor with regard to Controller's Personal Data; or (ii) Processor will take the corrective steps requested by Controller in its objection (which remove Controller's objection) and proceed to use the Sub-Processor with regard to Controller's Personal Data; or (iii) Processor may cease to provide or Controller may agree not to use (temporarily or permanently) the particular aspect of the service that would involve use of the Sub-Processor with regard to Controller's Personal Data.

In the absence of such objection, Processor shall be deemed to be fully entitled to appoint such Sub-Processor.

9.3. Processor undertakes to impose on any Sub-Processor, by means of a contractually binding agreement between the parties, data protection obligations which are materially similar to those set out in Attachment 2, taking into account the specific data processing operations undertaken by the Sub-Processor, as the case may be.

9.4. Controller acknowledges the Sub-Processors listed in Attachment 3 process Personal Data in the provision of the Services and agrees to such appointment by entering into this DPA.

9.5. The Parties agree that the term 'Sub-Processor(s)' refers only to service providers which provide data processing services in a capacity of processor. They further agree that this term shall not apply to the contractual service providers which provide ancillary services and which Processor may have recourse to in the provision of the Services under the Main Services Agreement, such as, without limitation, telecommunication services, postal services, office maintenance services, etc.

ARTICLE 10 - CONFIDENTIALITY

10.1. Processor confirms that all personnel who are processing Personal Data are subject to a confidentiality duty.

ARTICLE 11 - DURATION AND TERMINATION

11.1. This DPA is entered into for the duration of the Main Services Agreement. In the absence of a specified duration, this DPA shall be in force for the duration of the relationship between the Parties.

11.2. This DPA may be terminated by either Party, together with the Main Services Agreement, by giving appropriate notice for the termination of both agreements. In case of expiry or termination of the Main Services Agreement for any reason whatsoever, this DPA shall automatically terminate on the same date, and vice-versa.

11.3. After the provision of the Services related to Personal Data processing have come to an end, the Parties agree that Processor shall in principle delete Controller's Personal Data as soon as is reasonably possible and shall provide, upon Controller's request, a written confirmation of such deletion, the Personal Data processed on behalf of Controller. Alternatively, upon separate written agreement between the Parties, and in any case prior the expiry or termination date of the Main Services Agreement, Controller may request a copy of its Personal Data against payment of the reasonable costs incurred by Processor to render such service. It is understood by the Parties that the copy of the Personal Data may only contain data which Processor is legally and contractually permitted to provide, taking into account in particular the contractual provisions of third party content providers, social networks' terms of service and copyright laws.

Notwithstanding the foregoing, Processor shall be entitled to retain a copy of the Personal Data as long as required for evidentiary or statutory record retention purposes.

ARTICLE 12 – MISCELLANEOUS

12.1. This DPA together with its Attachments 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 the Parties with respect to its subject matter. In particular, the provisions of the general terms and conditions of Processor relating to data protection and the storage of data are void and shall be replaced by the provisions of this DPA and its Attachments.

12.2. This DPA may be amended only by a written instrument which specifically refers to this DPA. Processor shall be entitled to amend this DPA by providing thirty (30) days' prior written notice to Controller. In particular, Attachments 2, 3 and 4 to this DPA may be amended from time to time by Processor at its discretion by providing thirty (30) days' prior written notice, provided also that:

- Attachment 2 may not be modified in a manner that would materially and knowingly modify the level of protection of Personal Data ensured by the technical and organizational measures put in place in accordance with such Attachment 2 as of the effective date of this DPA;

- Attachment 3 may be modified in accordance with Article 9.2 of this DPA.

12.3. Each Party shall give all notices and communications to the other Party in writing including by e-mail.

12.4. Governing law and place of jurisdiction:

12.4.1 Where the Main Service Agreement has been executed with Talkwalker Sàrl, the validity, interpretation, and performance of this DPA shall be governed by the laws of the Grand-Duchy of Luxembourg, without giving effect to conflicts of law principles that may result in the application of the substantive laws of another jurisdiction. Any action, proceeding or claim arising out of or relating in any way to this DPA shall be brought and enforced in the courts of the judicial district of Luxembourg-City, Grand-Duchy of Luxembourg, which shall have exclusive jurisdiction.

12.4.2 Where the Main Service Agreement has been executed with Talkwalker Inc., the validity, interpretation, and performance of this DPA shall be governed by the laws of the State of New York, USA, without giving effect to conflicts of law principles that may result in the application of the substantive laws of another jurisdiction. Any action, proceeding or claim arising out of or relating in any way to this DPA shall be brought and enforced in the courts of the judicial district of the State of New York, USA, which shall have exclusive jurisdiction.

ATTACHMENT 1

NATURE AND PURPOSES OF THE DATA PROCESSING

The nature of data processing consists of collecting, sorting, saving, transferring, restricting and deleting Personal Data in the context of Controller's use of the Talkwalker Platform and Services.

The purposes of the data processing concern:

A – Controller's users' access to the Talkwalker Platform and Services based on such Controller's users' personal data provided by Controller to Processor for the purpose of defining Controller's users' accesses the Talkwalker Platform (processed data includes identification, authentication, login, access and audit trail data)

B – Controller's brand monitoring results processed on the basis of Controller's specific searches and, if applicable, the personal data input by the Customer in the Talkwalker Platform for the purposes of Controller's 360° internet media review, including brand monitoring, social media and web media listening and analytics, customer care and support

CATEGORIES OF PERSONAL DATA AND OF DATA SUBJECTS

A – Data provided by the Controller to the Processor relating to users appointed by the Controller to access to the Talkwalker Platform

Data type	Personal Data	Purpose of use	Non-Personal Data
User settings	IP address, cookies	Keep login session, analytics	
Talkwalker service settings	First and last name, email address, role of employee	Politeness, security, authentication, subscription to marketing communications (possible to unsubscribe)	Company name, Industry sector, Field of expertise, Access right level, Talkwalker settings (e.g. topics, queries), Time zone
	OAuth credentials and user IDs/nicknames of external connected services (Google, Twitter, Facebook…).	Optional and subject to specific consent (screen). Used in order to fetch the data, or an alternative way to authenticate users into Talkwalker.	Hash of Talkwalker login password (no storage of plain text passwords). In case Customer uses an SAML 2.0 integration, no hashes/passwords need to be stored by Talkwalker
Private insights	As defined by the customer, typically same as Author Data (next section)	Optional	Data uploaded by the user through the API or the web interface
Talkwalker service Alerts and Reports	Recipient email address	Necessary to establish communication	Talkwalker stores a history of the last alerts/reports sent to Customers
Exchange of email communication and support requests	Sender email addresses (or telephone numbers)	Necessary to establish communication	Email server IP addresses
	Identification elements typically present in email footer/signatures	Optional	Description of the issue, requests
Webserver log files	IP address, username	Incident investigation (typically abuse), capacity planning	Resource accessed, timestamp
Talkwalker service billing information	First and last name, email address, IP address when subscription was signed as part of signing proof (electronic signature), telephone number, history of bills.	Compliance with legal and corporate governance obligations and good practice	Detailed information about the Customer (VAT information) service provided (start and end dates, fees, payment dates), complete billing address

B – Author data related to the Controller's monitoring of brands via the publications made in the internet, including social media users.

Results provided by the Talkwalker Platform or API to the Controller to match Controller's Queries in the Talkwalker Platform. Processor only processes information which has been made public by the data subject himself, such as:

- Identification data (name, username, user id, geographical area);
- Personal characteristics (age, gender, status);
- Consumer habits;
- Hobbies and interests;
- Professional and educational background;
- Pictures and videos;
- Any other brand monitoring related information published by the data subject on a public Internet website or on a third-party platform that provides the Processor with data.

ATTACHMENT 2

TECHNICAL AND ORGANISATIONAL MEASURES
(cf. Articles 28 and 32 of the GDPR)

A – Confidentiality

- Employees
  - All staff working for Talkwalker are bound by confidentiality obligations pursuant to their employment agreement
  - Background checks
- Physical access control
  - Datacenters
    - Electronic physical entry control system with log
    - High security perimeter fencing around the entire data center park
    - Data center staff present 24/7
    - Video monitoring at entrances and exits; security door interlocking systems and server rooms
    - For people outside of the employment of the datacenter provider (data center visitors), entrance to the building is only permitted in the company of an employee from the datacenter provider
    - Fire and intrusion alarms
  - Talkwalker worldwide offices
    - Electronic physical entry control system with log
    - Service providers intervening on the site need to be accompanied by an employee or bound by a non-disclosure agreement
    - Fire and intrusion alarms
- Electronic access control
  - Production server administration
    - Dedicated servers fully managed by Talkwalker (no hypervisor or virtualization);
    - Three-factor authentication for production server administration: source IP address filtering, personal private public authentication key stored in computers with access to production and personal passphrase
    - Computers accessing the production connected to a dedicated and restricted network
  - Production access via the platform
    - Logical segregation of data between customers
    - Ability for the customer to manage their users and detailed access rights
    - Access to customer data by Talkwalker on a need-to-know basis, e.g. Sales representatives, Account managers, Finance department.
    - Talkwalker employees log into the platform using an internal Single Sign On (SSO) using 2-factor authentication. Customers can also link the access to their internal SSO (e.g. Active Directory) using SAML 2.0.
  - Regular review of access rights

- Management of media
    - Datacenters
        - Full disk encryption using AES-128 algorithms for all production servers hosting non-public Personal Data
        - Drives that were in operation on canceled servers will be swiped multiple times (deleted) by hosting provider in accordance with data protection polices
        - Defective drives that cannot be securely deleted shall be destroyed (shredded) directly in the datacenter
    - Workstations
        - Full disk encryption using AES-128 algorithms for mobile workstations used by Talkwalker employees

B – Integrity

- Data transfer control
    - Customers access the Talkwalker platform using state of the art HTTPS/TLS
    - All employees are trained in accordance with GDPR
    - Deletion of data in accordance with data protection regulations after termination of the DPA
- Data input control
    - Data is entered, collected and can be visualized by the Controller on the Talkwalker platform
    - Changes in data by customer and Talkwalker employees are logged in a separate dedicated audit log system. Logs can be provided to customers.
- Secure infrastructure and development
    - Internal development guidelines
    - Internal developer talks
    - Regular training of developers and engineers
    - Passwords are mixed with a dynamic salt and hashed, i.e. plain-text passwords are not kept
    - Network segregations at both datacenter (production vs. test) and office (Wireless vs. development vs access to production)

C – Availability and Resilience

- Hosting providers
    - Processing and hosting of Controller data takes place in dedicated infrastructures, holding a valid ISO 27001:2013 certificate;
- Availability control
    - Backup and recovery concept with daily backups of all customer data to a datacenter located in a remote location
    - Replication of services to account for the most common hardware failures
    - 24 hours monitoring and alerting of all servers and services
    - Employment of an uninterruptible power supply system or emergency power supply system
    - DDoS protection
- Protection against threats
    - Professional employment of security programs including both network-based and host-based firewalls
    - Network and server configurations are security-hardened
    - Virus and malware protection by default with automatic update of definitions and signatures
- Rapid recovery measures
    - 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
    - Talkwalker has Business Continuity and Disaster Recovery procedures to accelerate and standardize recovery works

D – Regular testing, assessment, evaluation and improvement

- Talkwalker has appointed a Data Protection Officer (dpo@talkwalker.com) and an Information Security Officer (security@talkwalker.com), reporting to the Talkwalker Board.
- Talkwalker has dedicated staff in order to implement and apply an Information Security Management System aligned with the international standard ISO27001:2013.
- Talkwalker has an Incident Management Procedure in place covering security and data protection issues that may arise and include escalation procedures in case notifications to data subjects, customers or authorities are required
- Talkwalker regularly mandates an independent organization to perform intrusion tests on the Talkwalker platform
- Talkwalker has written agreements with its Sub-Processors in order to ensure that Talkwalker obligations are replicated to them in accordance with this DPA. Before engaging a new sub-processor, Talkwalker carries out security and data protection risk assessment, which are proportionate to the sensitivity of the data handled by the Sub-Processor, except in the events where the Sub-Processor owns an independent security certification on which Talkwalker shall rely.

ATTACHMENT 3

LIST OF SUB-PROCESSORS

Recipient	Country	Purpose/Activity	Guarantees/Notes
Hetzner Online GmbH	European Union (Germany)	Hosting of Talkwalker platform	ISO/IEC 27001 certification DPA under GDPR Art 28
MailChimp (The Rocket Science Group LLC)	Unites States	Ensure deliverability of emails	DPA under GDPR Art 28 Privacy Shield certification (This sub-processor is not used when customer provides its own SMTP email server credentials)
Trendiction SA	European Union (Luxembourg)	IT support, billing, accounting Search, crawling, indexing of public data for brand monitoring purposes	Parent company of Talkwalker
Talkwalker Sarl	European Union (Luxembourg)	Compliance, Marketing, Consulting, Customer Success Management, Professional Services	Subsidiary (This sub-processor applies only to customers signing with Talkwalker Inc and not with Talkwalker Sarl)
Talkwalker GmbH	European Union (Germany)	Consulting, Customer Success Management, Professional Services	Subsidiary This sub-processor applies only to customers who are directly in touch with it.

RELEVANT ANCILLARY SUB-PROCESSORS

Recipient	Country	Purpose/Activity	Guarantees/Notes
Google LLC	Unites States	Email provider (Gmail), file hosting (Google Drive), and web analytics (Google Analytics)	DPA under GDPR Art 28 Privacy Shield certification
Salesforce.com Inc	Unites States	Sales pipeline and support Management of support requests sent by the customer	DPA under GDPR Art 28 Privacy Shield certification

ATTACHMENT 4

ADDENDUM TO THE DATA PROCESSOR AGREEMENT ("DPA")
"STANDARD EXPORT TERMS" FOR EXPORT
OF PERSONAL DATA OUTSIDE OF THE EUROPEAN UNION

These terms are only applicable in case clause 7.2 of the DPA applies

These Standard Export Terms are entered into between the Parties as defined hereunder in the context of the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (hereinafter "General Data Protection Regulation" or "GDPR") based on the EC Standard Contractual Clauses that were formerly required by Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection which no longer is effective as of May 25, 2018 (hereinafter "Standard Export Terms" or "Terms"). Considering these specific circumstances and in particular the GDPR rules, the Standard Contractual Clauses have been adapted into the present Standard Export Terms.

Name of the data exporting organisation (Customer): Controller as defined in the DPA (together the **data exporter**)

And

Name of the data importing organisation: Processor as defined in the DPA (the **data importer**)

each a 'party'; together 'the parties',

HAVE AGREED that these Terms shall apply to the transfer of personal data by Processor to Controller to the extent Controller or the affiliates designated by Controller to receive or access personal data are established in countries outside of the European Union which do not provide for an adequate level of protection under GDPR.

HAVE AGREED on the following Standard Export Terms in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in the Data Processor Agreement agreed between the Parties in the context of the GDPR (hereinafter "DPA").

Clause 1 **- Definitions**

For the purposes of the Standard Export Terms:

(a) 'personal data' has the meaning as set out in the GDPR and in the DPA and its attachments;

(b) 'the data exporter' means the controller who transfers the personal data;

(c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Standard Export Terms and who is not subject to a third country's system ensuring adequate protection within the meaning of the GDPR;

(d) 'the sub-processor' means any processor engaged by the data who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Standard Export Terms and the terms of the written subcontract;

(e) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2 **- Details of the transfer**

The details of the transfer and in particular the categories of personal data are described in these Terms, in the DPA and in the Main Services Agreement, taking into account that the transfer concerns the making available of personal data to the data exporter and its affiliates that are bound by the Main Services Agreement.

Clause 3**- Third-party beneficiary clause**

1. The data subject can enforce against the data exporter these Standard Export Terms as third-party beneficiary with respect to the obligations that are incumbent to it.

2. The data subject can enforce against the data importer these Standard Export Terms as third-party beneficiary with respect to the obligations that are incumbent to it.

Clause 4 **- Obligations of the data exporter**

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection laws (including GDPR) and does not violate their relevant provisions;

(b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Terms;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures as specified in Attachment 2 of the DPA;

(d) that after assessment of the requirements of the applicable data protection laws, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) to forward any notification received from the data importer or any sub-processor to the data protection supervisory authority to the extent as required by applicable law;

(g) to make available to the data subjects upon request a copy of the Terms, with the exception of Attachments 2 and 3 of the DPA, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Terms, unless the Terms or the contract contain commercial information, in which case it may remove such commercial information;

(h) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 10 by a sub-processor providing a level of protection for the personal data and the rights of data subject that is materially similar to that applied by the data importer under the Terms;

(i) that it will ensure compliance with Clause 4(a) to (j); and

(j) that it will inform importer in due course and at the latest at the date of execution of the Main Services Agreement of potential obligations specific to the data privacy laws applicable in its jurisdiction.

***Clause 5*- Obligations of the data importer**

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter in compliance with its instructions and the Terms;

(b) that it has implemented the technical and organisational security measures specified in the DPA;

(c) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

(ii) any accidental or unauthorised access; and

(iii) any request received directly from the data subjects unless it has been otherwise authorised to do so;

(d) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(e) at the request of the data exporter, and in accordance with the terms of the DPA, to submit its data-processing facilities for audit of the processing activities covered by the Terms which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(f) to make available to the data subject upon request a copy of the Terms, unless the Terms or contract contain commercial information, in which case it may remove such commercial information, with the exception of Attachments 2 and 3 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(g) that, in the event of sub-processing, it has previously informed the data exporter and obtained a general authorization in compliance with Article 28 3° of the GDPR and the DPA;

(h) that the processing services by the sub-processor will be carried out in accordance with Clause10.

Clause 6 **– Liability**

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 10 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 10, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

Clause 7 **- Mediation and jurisdiction**

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Standard Export Terms, the data importer will accept the decision of the data subject:
   a) to refer the dispute to mediation by the supervisory authority;
   b) to refer the dispute to the competent courts as set out in the DPA.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8 **- Cooperation with supervisory authorities**

The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

Clause 9 **- Governing law**

The Standard Export Terms shall be governed by the law designated in the DPA.

Clause 10 **- Sub-processing**

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under these Standard Export Terms without the general authorisation provided

by the data exporter in line with Article 28 3° of the GDPR and the DPA. Where the data importer subcontracts its obligations under the Standard Export Terms, in the above-mentioned conditions, it shall do so only by way of a written agreement with the sub-processor which imposes materially similar obligations on the sub-processor as are imposed on the data importer under the DPA. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

2. The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State of the sub-processor or in the event where the sub-processor is not located in an EU Member State by the law as designated in the DPA.
3. The data exporter shall keep a list of sub-processing agreements concluded under these Standard Export Terms and notified by the data importer pursuant to the DPA, which shall be updated at least once a year.

Clause 11 **- Obligation after the termination of personal data-processing services**

1. The parties agree that on the termination of the provision of data-processing services, the data importer shall, either return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data in accordance with Article 11.3 of the DPA. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred any more.
2. The data importer warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

End of Document