TALKWALKER DATA PROCESSING ADDENDUM

This Data Processing Addendum, including its Appendices ("**DPA**"), forms part of the applicable Terms of Service or other agreement (the "**Agreement**") between **Talkwalker S.à r.l.** (33 avenue John F. Kennedy, L-1855, Luxembourg), **Talkwalker Inc.** (3616 Far West Blvd., Suite 117 #419, Austin, TX 78731), **Talkwalker Pte. Ltd.** (9, Raffles Place, #26-01 Republic Plaza, Singapore 048619), **Talkwalker KK** (Ark Hills South Tower 16F, 1-4-5 Roppongi, Minato-ku Tokyo, 13, 106-0032, Japan), or **Talkwalker India Private Limited** (WeWork Enam Sambhav, (Office 03A-121) 3rd Floor, C-20, G Block, BKC, Mumbai, Mumbai City, Maharashtra, India, 400051) (as applicable) (together referred to as "**Talkwalker**") and the entity identified as Customer in the Agreement ("**Customer**").

In the course of providing the Services to Customer pursuant to the Agreement, Talkwalker may Process Customer Personal Data (as defined below) on Customer's behalf. This DPA sets out the terms that apply when Customer Personal Data that is subject to Applicable Data Protection Laws is Processed by Talkwalker on Customer's behalf under the Agreement.

Customer enters into this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Affiliates that are permitted to use the Services under the Agreement, and the Talkwalker entity that is party to the Agreement is party to this DPA. Unless otherwise defined herein, capitalized terms in this DPA will have the same meaning ascribed to them in the Agreement.

1. PROCESSING OF PERSONAL DATA

1.1 **Scope.** This DPA applies to the Processing of Customer Personal Data that is subject to Applicable Data Protection Laws by Talkwalker in its capacity as a processor or service provider for the purpose of providing the Services. This DPA does not apply to personal data or personal information that Customer Processes via Third-Party Services.

1.2 **Roles.** The parties acknowledge and agree that, with regard to the Processing of Customer Personal Data, Customer is the controller or business and Talkwalker is Customer's processor or service provider under Applicable Data Protection Laws.

1.3 **Details of Processing.** The subject matter, duration, nature, and purpose of the Processing, and the types of personal data or personal information, and categories of data subjects or consumers, are described in **Appendix 1** of this DPA.

1.4 **Customer's Responsibilities.** Customer shall, in its use of the Services: (a) comply with its obligations as a controller or business and Process Customer Personal Data in accordance with Applicable Data Protection Laws; (b) ensure that its instructions to Talkwalker comply with Applicable Data Protection Laws; (c) have sole responsibility for the accuracy, quality, and legality of Customer Personal Data; and (d) ensure that Customer is entitled to transfer Customer Personal Data to Talkwalker so that Talkwalker and its Subprocessors may lawfully Process Customer Personal Data under Applicable Data Protection Laws.

1.5 **Customer's Instructions**. Customer instructs Talkwalker to collect, analyze, display, store and otherwise Process Customer Personal Data for the purpose of providing, updating, and improving the Services to Customer in a manner consistent with the Agreement, this DPA and where applicable the privacy policy published at https://www.hootsuite.com/legal/privacy. Talkwalker will comply with other reasonable instructions provided by Customer (e.g., via email or support tickets) or initiated by Customer's authorized users of the Services where such instructions are consistent with the terms of the Agreement. Talkwalker will inform Customer if, in its opinion, an instruction infringes Applicable Data Protection Laws.

1.6 **Talkwalker's Responsibilities.** Talkwalker shall comply with its obligations under Applicable Data Protection Laws in its role as a processor or service provider and notify Customer if it cannot or can no longer meet its obligations. Talkwalker will only Process Customer Personal Data in accordance with Customer's documented instructions as set out in Section 1.5 and agrees that it shall not: (a) "sell" or "share" Customer Personal Data within the meaning of Applicable Data Protection Laws (including the CCPA); (b) retain, use, or disclose Customer Personal Data for any purpose other than the business purposes specified under the Agreement; (c) use Customer Personal Data received in connection with the Agreement outside of the relationship between Customer and Talkwalker; or (d) combine Customer Personal Data with information that Talkwalker has received from other sources; in each case except as permitted under the Agreement and Applicable Data Protection Laws.

2. SUB-PROCESSORS

2.1 **Appointment of Subprocessors**. Customer agrees and provides a general written authorization that Talkwalker and its Affiliates may engage Subprocessors, provided that: (a) Talkwalker and each Subprocessor shall enter a

written agreement containing data protection obligations that provide an equivalent level of protection for Customer Personal Data as those described in this DPA (in particular, providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of Applicable Data Protection Laws); and (b) Talkwalker shall remain responsible for its Subprocessors' compliance with the obligations under this DPA and for any acts or omissions of its Subprocessors that causes Talkwalker to breach any of its obligations under this DPA.

2.2 **Identification and Notification of Authorized Subprocessors.** Talkwalker maintains a list of its authorized Subprocessors at a publicly listed web page, currently found at https://hootsuite.com/legal/subprocessor-list. Customer may subscribe to receive notifications of new or replacement Subprocessors by emailing privacy@hootsuite.com with the subject "Talkwalker Subprocessor Subscribe". If Customer subscribes to receive notifications, Talkwalker shall provide thirty (30) days' notification of any intended new or replacement Subprocessor before authorizing such Subprocessor to Process Customer Personal Data in connection with the provision of the applicable Services.

2.3 **Right to Object to New Subprocessors.** Customer may reasonably object to Talkwalker's use of a new or replacement Subprocessor by notifying Talkwalker promptly in writing within ten (10) business days after receipt of Talkwalker's notice in accordance with Section 2.2. Customer shall explain the reasonable grounds for any such objection, which must relate to compliance with Applicable Data Protection Laws. Upon receipt of an objection, Talkwalker will use reasonable efforts to make available to Customer a change in the Services or recommend a commercially reasonable change to Customer's configuration or use of the Services to avoid the Processing of Customer Personal Data by the objected-to Subprocessor. If Talkwalker is unable to make such a change or recommendation within a reasonable period of time, Customer may terminate the affected part of the Services in accordance with the terms of the Agreement.

3. CONFIDENTIALITY

3.1 **Confidentiality.** Talkwalker shall ensure that any persons that it authorizes to Process Customer Personal Data (including its staff, agents, and contractors) shall be subject to a duty of confidentiality that survives the termination of their employment and/or contractual relationship.

3.2 **Government requests.** Talkwalker shall not disclose Customer Personal Data to any law enforcement agency or government authority (collectively, "**Government Authority**") unless instructed by Customer, or as necessary to comply with applicable laws or a valid and binding order of a Government Authority, such as a subpoena or court order. If a Government Authority requests access to Customer Personal Data, and unless legally prohibited from doing so, Talkwalker shall (a) inform the Government Authority that Talkwalker is a processor or service provider and attempt to redirect the Government Authority to Customer (and may provide Customer's basic contact information to the Government Authority for these purposes); and (b) in the event such redirection is not possible, notify Customer of the request to allow Customer to seek a protective order or other appropriate remedy. If Talkwalker is legally compelled to respond to the request, Talkwalker shall review the legality of the request and determine whether the request may be challenged. In any event, Talkwalker shall only disclose the minimum information that is required to comply with the request.

4. SECURITY

4.1 **Security Measures.** Talkwalker shall implement and maintain appropriate technical and organizational measures to protect Customer Personal Data from Security Incidents and preserve the security, confidentiality, and integrity of Customer Personal Data, as further described in **Appendix 2** of this DPA ("**Security Measures**"). These Security Measures shall include, as appropriate: (a) the pseudonymization and encryption of Customer Personal Data; (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of Talkwalker's systems and services; (c) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing. Talkwalker may update or modify the Security Measures from time to time provided that such updates and modifications do not materially decrease the overall security of the Services provided to Customer.

4.2 **Audits and Third-Party Security Certifications**. Talkwalker uses external auditors to verify the adequacy of its Security Measures and agrees to having an audit performed: (a) annually; (b) according to AICPA SOC 2 (AT-101) or substantially similar requirements; and (c) by independent third-party security professionals at Talkwalker's selection and expense. Customer agrees that Talkwalker's audit reports and certifications will be used to satisfy any audit or inspection requests by Customer (or Customer's independent, third-party auditor), including for the

purposes of meeting any audit obligations under Applicable Data Protection Laws or the SCCs, which Talkwalker will make available to Customer upon written request no more than once per year and subject to the confidentiality obligations set forth in the Agreement (or a separate non-disclosure agreement, if necessary).

5. INCIDENT MANAGEMENT AND NOTIFICATION

5.1 If Talkwalker becomes aware of a Security Incident for which notification to Customer is required under Applicable Data Protection Laws, Talkwalker will, without undue delay, notify Customer of the Security Incident. Talkwalker will include in the notification such information about the Security Incident as Talkwalker is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to Talkwalker, and any restrictions on disclosing the information, such as confidentiality. Any notice of a Security Incident provided by Talkwalker is not, and will not be construed as, an acknowledgement by Talkwalker of any fault or liability.

6. RIGHTS REQUESTS

6.1 To the extent required under Applicable Data Protection Laws, and insofar as Customer cannot respond through functionality made available via the Services, Talkwalker shall provide Customer with commercially reasonable assistance to enable Customer to respond to requests from data subjects or consumers seeking to exercise their rights under Applicable Data Protection Laws, taking into account the nature of the Processing.

7. DATA PROTECTION IMPACT ASSESSMENTS

7.1 **Data Protection Impact Assessments.** Upon Customer's reasonable written request, and to the extent required under Applicable Data Protection Laws, Talkwalker shall provide Customer with reasonable cooperation and assistance needed to fulfill Customer's obligation to carry out data protection impact assessments and consult with supervisory authorities related to Customer's use of the Services.

8. INTERNATIONAL DATA TRANSFERS

8.1 **International Data Transfers.** Customer acknowledges and agrees that Talkwalker may transfer and Process Customer Personal Data outside Europe as necessary to provide the Services, including Canada and the United States and other countries where Talkwalker, its Affiliates, and Subprocessors maintain data processing operations. Talkwalker shall take all such measures as are necessary to ensure such transfers are made in compliance with applicable European Data Protection Laws.

8.2 **Standard Contractual Clauses.** To the extent that the transfer of Customer Personal Data from Customer to Talkwalker involves a Restricted Transfer, then the SCCs shall be incorporated and form an integral part of this DPA, with Customer (and any Customer Affiliates) as the "data exporter" and the applicable Talkwalker entity as the "data importer", as follows:

(a) In relation to Customer Personal Data that is subject to the GDPR: (i) Module Two (controller to processor) will apply; (ii) in Clause 7, the optional docking clause shall apply; (iii) in Clause 9, Option 2 will apply, and the time period for prior notice of Subprocessor changes shall be as set out in Section 2.2 of this DPA; (iv) in Clause 11, the optional language will not apply; (v) in Clause 17, Option 1 will apply, and the SCCs will be governed by Irish law; (vi) in Clause 18(b), disputes shall be resolved before the courts of Ireland; (vii) Annex I of the SCCs shall be deemed completed with the information set out in Appendix 1 to this DPA; and (viii) Annex II of the SCCs shall be deemed completed with the information set out in Appendix 2 to this DPA.

(b) In relation to Customer Personal Data that is subject to the UK GDPR, the SCCs shall apply in accordance with Section 8.2(a), with the following modifications: (i) the SCCs shall be deemed amended as specified by the UK Addendum, which shall be deemed executed by the parties and incorporated into and form an integral part of this DPA; (ii) any conflict between the SCCs and the UK Addendum shall be resolved in accordance with Section 10 and Section 11 of the UK Addendum; (iii) tables 1 to 3 in Part 1 shall be completed respectively with the information set out in Appendices 1 and 2 of this DPA; and (iv) table 4 in Part 1 shall be deemed completed by selecting "neither party".

(c) In relation to Customer Personal Data that is subject to the Swiss FADP, the SCCs shall apply in accordance with Section 8.2(a), with the following modifications: (i) references to "Regulation (EU) 2016/679" and specific articles therein shall be replaced with references to the Swiss FADP and the equivalent articles or sections therein; (ii) references to "EU", "Union" and "Member State" shall be replaced with references to "Switzerland"; (iii) Clause 13(a) and Annex II(C) are not used and the "competent supervisory authority" shall be the Swiss Federal Data Protection Information Commissioner; (iv) references to the "competent

supervisory authority" and "competent courts" shall be replaced with references to the "Swiss Federal Data Protection Information Commissioner" and "applicable courts of Switzerland"; (v) in Clause 17, the SCCs shall be governed by the laws of Switzerland; and (vi) in Clause 18(b), disputes shall be resolved before the applicable courts of Switzerland.

8.3 **Clarifications to the Standard Contractual Clauses.** The parties further agree that if Talkwalker cannot ensure compliance with the SCCs, it shall promptly inform Customer and Customer shall provide Talkwalker with a reasonable period of time to cure the non-compliance, during which time Talkwalker and Customer shall reasonably cooperate to agree what additional safeguards or measures, if any, may be reasonably required. Customer shall only be entitled to suspend the transfer of Customer Personal Data and/or terminate the affected parts of the Services for non-compliance with the SCCs if Talkwalker has not or cannot cure the non-compliance before the end of the cure period. It is not the intention of either party to contradict or restrict any of the provisions set forth in the SCCs and, accordingly, if and to the extent the SCCs conflict with any provision of the Agreement (including this DPA) the SCCs shall prevail to the extent of such conflict.

9. RETURN AND DELETION OF PERSONAL DATA.

9.1 Upon termination of the Services, Talkwalker shall, upon Customer's written request received by Talkwalker within 30 days of termination of the Services, return or delete all Customer Personal Data and copies of such data in its custody or control, unless it is legally required to retain the Customer Personal Data. Until the Customer Personal Data is deleted or returned, Talkwalker shall continue to protect the Customer Personal Data in accordance with the Agreement, this DPA, and Applicable Data Protection Laws.

10. GENERAL PROVISIONS

10.1 **Legal Effect.** This DPA is an addendum to and is incorporated into the Agreement between Customer and the Talkwalker entity that is party to the Agreement. Except for changes made by this DPA, the Agreement remains unchanged and in full force and effect. This DPA supersedes and replaces all prior or contemporaneous representations, understandings, agreements, or communications between Customer and Talkwalker, whether written or verbal, regarding the subject matter of this DPA, including any data processing addenda previously entered into between Talkwalker and Customer.

10.2 **Conflict.** If there is a conflict between any provision in this DPA and any provision in the Agreement, this DPA controls and takes precedence to the extent of such conflict.

10.3 **Counterparts.** This DPA may be executed in any number of counterparts, each of which will be deemed to be an original and all of which taken together will comprise a single instrument. This DPA may be delivered by electronic document format (e.g., PDF, Adobe Sign or DocuSign), and electronic copies of executed signature pages are binding as originals.

10.4 **Termination.** This DPA shall continue in force until the termination of the Agreement.

10.5 **Limitations of Liability**. The liability of each party under this DPA (including the SCCs) shall be subject to the exclusions and limitations of liability set out in the Agreement. In no event does this DPA restrict or limit the rights of any data subject or consumer under Applicable Data Protection Laws or the SCCs.

10.6 **Disclosure of this DPA.** Customer acknowledges that Talkwalker may disclose this DPA and any relevant privacy provisions in the Agreement to a European supervisory authority, or any other European, Canadian, or US judicial or regulatory body upon request.

11. DEFINITIONS

11.1 In this DPA, the following terms have the meanings given to them below:

(a) The terms "**business**", "**consumer**", "**controller**", "**data subject**", "**personal data**", "**personal information**", "**processor**", "**service provider**", and "**supervisory authority**" have the meanings given to them under Applicable Data Protection Laws.

(b) "**Applicable Data Protection Laws"** means European Data Protection Laws, US Privacy Laws, and all other data protection and privacy laws and regulations as applicable to the Processing of Customer Personal Data under the Agreement.

(c) "**Customer Personal Data**" means any personal data or personal information provided by (or on behalf of) Customer to Talkwalker, or otherwise Processed by Talkwalker on Customer's behalf under the

Agreement, as described in **Appendix 1** of this DPA.

(d) **"Europe"** means, for the purposes of this DPA, the European Economic Area and its Member States, Switzerland and the United Kingdom ("**UK**").

(e) **"European Data Protection Laws**" means all data protection and privacy laws and binding regulations of Europe that are applicable to the Processing of Customer Personal Data under the Agreement, including: (i) the EU General Data Protection Regulation ("**GDPR**"); (ii) any applicable national implementations of the GDPR; (iii) the GDPR as it forms part of UK law by virtue of Section 3 of the European Union (Withdrawal) Act 2018 and the Data Protection Act 2018 (together, the "**UK GDPR**"); and (iv) the Swiss Federal Act on Data Protection Act of 2020 and its Ordinance ("**Swiss FADP**"); in each case as may be amended, superseded or replaced from time to time.

(f) **"Process"** or **"Processing"** means any operation or set of operations that are performed on Customer Personal Data, whether or not by automated means, including the collection, use, and disclosure of Customer Personal Data.

(g) **"Restricted Transfer"** means a transfer of Customer Personal Data originating from Europe to a country that does not provide an adequate level of protection for personal data within the meaning of applicable European Data Protection Laws.

(h) **"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Personal Data Processed by Talkwalker in connection with the provision of the Services. This does not include unsuccessful attempts or activities that do not compromise the security of Customer Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.

(i) **"Services"** has the same meaning given to it in the Agreement.

(j) "**SCCs**" means the standard contractual clauses as approved by the European Commission pursuant to its decision 2021/914 of 4 June 2021, as may be amended, superseded, or replaced from time to time.

(k) "**Subprocessor**" means any third-party processor engaged by Talkwalker or its Affiliates to assist in providing the Services to Customer in accordance with the Agreement and this DPA. Subprocessors do not include Talkwalker's or its Affiliates' employees, contractors, or consultants.

(l) "**UK Addendum**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner under section 119A(1) of the Data Protection Act 2018, as may be amended, superseded or replaced from time to time.

(m) "**US Privacy Laws"** means all United States federal and state privacy and data protection laws that are applicable to the Processing of Customer Personal Data under the Agreement, including without limitation: (i) the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and any implementing regulations relating to the same (together, the "**CCPA**"); (ii) the Virginia Consumer Data Protection Act ("**CDPA**"); (iii) the Colorado Privacy Act ("**CPA**"); (iv) the Utah Consumer Privacy Act ("**UCPA**"); and (v) the Connecticut Data Privacy Act ("**CTDPA**"); in each case when effective and as may be amended, superseded or replaced from time to time.

[Remainder of page intentionally left blank.]

Appendix 1: Description of the Processing

This Appendix describes the processing of Customer Personal Data by the parties in connection with the Services and forms an integral part of the Agreement. Unless otherwise defined herein, capitalized terms in this Appendix will have the same meaning ascribed to them in the Agreement.

(A) List of parties

Data Exporter:	
Name:	The data exporter is the entity identified as "Customer" in the Agreement.
Address:	The address is set out in the Agreement.
Contact person's name, position and contact details:	The contact information is as set out in the Agreement.
Activities relevant to data transferred under these Clauses:	Processing activities in receiving the Services as set forth in the Agreement
Role (controller / processor):	Controller

Data Importer:	
Name:	Talkwalker entity, as set out under Section 8 of the DPA and in the Agreement.
Address:	The address as set out in the Agreement.
Contact person's name, position and contact details:	Colin McGowan, Senior Legal Counsel, EMEA
Activities relevant to data transferred under these Clauses:	Processing activities in providing the Services as set forth in the Agreement
Role (controller / processor):	Processor

(B) Description of the processing & transfer

Services	
Categories of data subjects or consumers:	Social media and internet users — Individuals whose Personal Data is publicly available and collected from social media platforms and other public sources (e.g., Facebook, Instagram, LinkedIn, Global News Group, blogs, forums, etc.).
Categories of personal data or personal information:	The information that is processed through the Services is determined and controlled by Customers in their sole discretion and may include the following categories: ● Personal identification data (e.g., name, social media identifier, profile information) ● Contact details (e.g., name, email address) ● Identification data (e.g., name, username, user ID, geographical area) ● Social media and internet user generated content (e.g., status updates, comments, items on blog or forum containing keywords and characteristics ● Social media and internet users publicly-available personal characteristics (e.g., age,

	gender, interests and preferences, professional and educational background, photos and videos) ● Any other brand monitoring related information published on a publicly available social media or internet site that contains personal information
Sensitive data (if applicable) and applied restrictions or safeguards:	The information that is processed through the Services is determined and controlled by Customers and may include the following sensitive data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, data concerning health or sex life, or data relating to offenses, criminal convictions or security measures. See Appendix 2 for applied restrictions and safeguards for sensitive data.
Frequency of the transfer:	Continuous
Nature of the Processing:	Collection, storage, organization, modification, retrieval, disclosure, communication, and other uses in performance of the Services as set out in the Agreement.
Purpose(s) and subject matter of the transfer and further Processing:	Processing activities in performance of the Services as set out in the Agreement, including providing access to the Talkwalker platform and services.
Period and duration for which the personal data or personal information will be Processed and retained:	In accordance with Section 9 of the DPA.

(C) Competent supervisory authority

For the purposes of the SCCs, the competent supervisory authority shall be determined in accordance with the GDPR.

Appendix 2: Security Measures

This Appendix describes the technical and organizational measures to be implemented by Talkwalker and forms an integral part of the Agreement. Unless otherwise defined herein, capitalized terms in this Appendix will have the same meaning ascribed to them in the Agreement.

The technical and organizational measures ("**TOMs**") to be implemented by Talkwalker (including any relevant certifications) to ensure an appropriate level of security taking into account the nature, scope, context and purposes of the processing, and the risks for the rights and freedoms of natural persons, are described in the following table.

Type of TOMs	**Description of TOMs**
Measures of pseudonymisation and encryption of personal data	<u>Pseudonymisation</u> Processing of personal data is limited within the Services. For example, when data is being processed (e.g., retrieved and analyzed), and where feasible, a unique ID is used as an identifier rather than the full personal data fields such as account user's first and last name; and their business email address). <u>Encryption</u> Data provided by customers to Talkwalker is encrypted during transit and at rest to mitigate against security threats at industry standard levels.
Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services	<u>Access controls</u> ● Access control policies and procedures that address onboarding, off-boarding, transition between roles, regular access reviews, limitations and usage control of administrator privileges, and inactivity timeouts have been implemented. ● Identification and segregation of conflicting duties and areas of responsibility, such as separation of duties is implemented. ● A current and accurate inventory of computer accounts is maintained. ● The principles of 'need-to-know' and 'least privilege' are enforced and user access rights are reviewed on a regular basis to identify excessive privileges. ● A limit of login attempts is enforced. ● Remote access to production systems and other sensitive network segments require connection through a VPN. <u>Authentication</u> ● Passwords require a defined minimum complexity. Initial passwords must be changed after the first login. ● Access to the systems used by Talkwalker employees and contract personnel is controlled by multi-factor authentication (MFA). ● Single sign-on (SSO) has been implemented company-wide to ensure greater and more centralized access control to the systems used by Talkwalker employees and contract personnel. <u>Personnel practices</u> ● All employees are bound by confidentiality agreements and Talkwalker's security and privacy policies. Upon onboarding and at least annually thereafter, all employees receive security and privacy training. ● Pre-employment screening (which may include criminal background screening), commensurate with the sensitivity of the role, and where permissible by law, is conducted. <u>Intrusion Detection and Monitoring</u> ● Intrusion detection mechanisms are used to monitor the Services for unauthorized intrusions. ● Firewalls are configured according to industry best practices, and ports not utilized for delivery of the Talkwalker Services are blocked by configuration with our data center

	provider. ● Vulnerability scans are performed on production and commercially reasonable efforts are taken to remediate any findings that present a material risk to the Talkwalker environment. ● Screen lockouts are enforced and full disk encryption is implemented for company laptops.
Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident	<u>Disaster Recovery</u> Customer data is stored redundantly at multiple locations in Talkwalker's hosting provider's data centers to ensure availability; and there are backup and restoration procedures to allow recovery from a major disaster. <u>Backups</u> Customer Content and application source code is automatically backed up at least on a nightly basis. Talkwalker's operations team is alerted in the event of any failure with this system.
Processes for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures in order to ensure the security of the processing	<u>Security team</u> A dedicated Security leader and Security team oversees, monitors and tests the technical and organizational measures implemented for the Services. <u>Audits and Certifications</u> Talkwalker Services security related audits and certifications include: ● An annual SOC 2 Type II audit performed by an independent third-party to test the effectiveness of the technical and organizational measures in place.
Measures for user identification and authorization	<u>Logs</u> ● Logs that record details of transmissions of data from IT systems that store or process personal data and user access to the Services are monitored and reviewed by the Security team to verify authorized access. ● All system logs that contain important information, such as authentication, network access logs, etc. are collected in a central repository and monitored by a dedicated team for suspicious activity. <u>Encryption and Firewalls</u> ● All public facing interfaces are secured via industry standard encryption and firewalls. ● Production systems are only accessible after MFA. ● Firewalls (e.g., Web Application Firewall, Network Firewalls) are used and monitored continuously on production systems. <u>Access Control</u> ● Role-based access control is enforced in accordance with 'need-to-know' and 'least privilege' principles
Measures for the protection of data during transmission	The Services support the latest industry-standard secure cipher suites and protocols to encrypt all traffic in transit. Talkwalker currently supports TLS 1.2 or above on its web traffic. Remote access to production systems and some other sensitive network segments is only accessible via a VPN tunnel, which requires MFA and is end-to-end encrypted.
Measures for the protection of data during storage	Customer Content is encrypted at rest (using AES with 128 or 256-bit encryption), where appropriate and having regard to the nature of the content and associated risks. Access controls (as further described above) are implemented to restrict access only to authorized personnel on a 'need-to-know' and 'least privilege' basis for the purpose of maintaining the Services.
Measures for ensuring physical security of locations at which	<u>Cloud service provider security</u> Talkwalker uses Hetzner for its production data centers to provide its Services. Hetzner has the ISO 27001 certification.

personal data are processed	Talkwalker office security All Talkwalker offices where personal data may be processed have: ● Electronic access control systems to protect the main entry and security areas ● Monitoring of the facility by security services and access logging to the facility ● Video surveillance of security-relevant security areas, such as entrances and exits ● Central assignment and revocation of access authorisations ● Identification of all visitors by verification of their identity card and registration (a log of visitors is kept) ● Mandatory identification within the security areas for all employees and visitors ● Visitors must be accompanied by employees at all times.
Measures for ensuring events logging	All systems used in the provision of the Talkwalker Services, including firewalls, routers, network switches, intrusion detection systems, anti-malware services and operating systems, log information to secure log servers to enable security reviews and analysis. See also: Intrusion Detection and Monitoring above for more details
Measures for ensuring system configuration, including default configuration	Production servers, databases, and cloud security configurations are hardened in line with internal configuration guidelines and in accordance with the Configuration Management Policy. The configuration and builds of systems are managed in code via our Configuration Management Systems. Changes to configuration sets require peer review and approval. New instances are created from pre-configured and hardened 'base images'.
Measures for internal IT and IT security governance and management and Measures for certification/assurance of processes and products	Talkwalker implements and maintains industry-standard security policies and procedures that align with the National Institute of Standards and Technology (NIST) cybersecurity framework. There is a dedicated Security leader and team that implements the security policies and standards, and oversees annual audits and certifications as referenced above (for example, SOC 2 Type II).
Measures for ensuring data minimisation	Access to personal data is restricted on a 'need-to-know' and 'least privilege' basis. Data exporters (customers) are data controllers of the data they choose to upload onto the Services and may decide to limit the amount of data being processed. Access to production servers is controlled through role-based access controls.
Measures for ensuring data quality	Data is retrieved from social media networks in real-time using APIs and the data accuracy and quality will be dependent on the source data from the social networks. Data exporters (customers) are data controllers of the data they choose to upload onto the Services and may update or amend the data to ensure data quality.
Measures for ensuring limited data retention	A Records Retention and Destruction Policy is in place and data is retained as long as required to provide the Services, for record keeping purposes, to comply with legal obligations, resolve disputes, and enforce the terms for the Services. Data deletion processes are in place for data subject deletion requests.
Measures for ensuring accountability	A dedicated security leader and team is responsible for ensuring appropriate security and data protection policies and procedures are implemented and adhered to. Talkwalker has appointed a Data Protection Officer who, together with the Privacy team, oversees the privacy program. At the Executive level, leaders are regularly updated on data protection matters and may be

	involved in providing strategic input into Talkwalker's data protection practices. Employees undergo annual privacy and security training. A process has been implemented to promptly respond to and manage data subject requests, such as requests for access and deletion of their information. Talkwalker observes privacy by design principles, including conducting privacy impact assessments and reviews when implementing new product functionality, and new processes.
Measures for allowing data portability and ensuring erasure	Customers may request the return or deletion of all personal data and copies of such data in its custody or control. Processes are in place for data subject deletion requests. For data portability, there are "Data Exporting" options within the Services where Customer content may be exported into CSV formats.
Subprocessor Information	See: https://www.hootsuite.com/legal/subprocessor-list