# DATA PROCESSING ADDENDUM

This Data Processing Addendum (the "DPA") forms part of BrightTALK's Customer Agreement and any applicable Service Specific Terms or other mutually negotiated paperwork (the "Agreement") entered into by and between BrightTALK, Inc. and its subsidiaries and affiliates, including its parent company (collectively, "BrightTALK") and Client ("Client"). Capitalized terms not defined in this DPA shall have the meaning set forth in the Agreement. In the event of a conflict between the terms and conditions of this DPA and the Agreement, the terms and conditions of this DPA shall take precedence with regard to the subject matter of this DPA. This DPA sets forth the provisions applicable between the parties whether they act as Controllers of Licensed Data and/or to the extent that BrightTALK acts as a Processor of Client Personal Data. BrightTALK and Client are together referred to herein as the "Parties," or each may be referred to individually as a "Party."

## 1. Definitions.

"**Authorized Affiliate**" means a Client Affiliate explicitly permitted to use the Services pursuant to the Agreement.

"**Client Personal Data**" means personal data provided or made available by Client in connection with the Services and processed by BrightTALK or a sub-processor exclusively for Client.

**"CCPA"** means the California Consumer Privacy Act, as may be subsequently modified or amended, including by the California Privacy Rights Act ("CPRA"), together with any implementing regulations.

"**Data Protection Laws**" refers to all applicable data protection and privacy laws and regulations regarding the processing of personal data in connection with this DPA, including but not limited to, European Union or Member State laws with respect to personal data, including GDPR, and any other applicable data protection or privacy laws of any other country and state, including the CCPA.

"**EEA**" means the member states of the European Union, Iceland, Liechtenstein, and Norway.

"**GDPR**" means the General Data Protection Regulation, or Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons regarding the processing of personal data and on the free movement of such data and for the purpose of this DPA includes the corresponding laws of the United Kingdom (including the UK GDPR and Data Protection Act 2018); "**controller**," "**processor**," "**sub-processor**," "**data subject**," "**personal data**," "**personal data breach**," "**processing**," "**process,**" and "**Supervisory Authority**" each will have the meanings given in the GDPR.

"**Licensed Data**" means a member contact record that includes information regarding a business professional, including the individual's name, contact information, company affiliation, and other information made available to Client as part of the Services.

"**Processing Services**" means any and all Services provided by BrightTALK to Client under the Agreement that involve the processing of Client Personal Data.

## 2. Roles of the Parties.

This DPA applies when Client Personal Data is transferred to BrightTALK by Client and processed by BrightTALK strictly on behalf of Client, as part of BrightTALK's provision of the Services, where BrightTALK serves as a data processor and/or when personal data is transferred to Client by BrightTALK as part of the provision of the Services by BrightTALK to Client, including the delivery of Licensed Data, where the parties each serve as an independent controller.

## 3. Processing Details and Obligations.

(a) With respect to the processing of Client Personal Data and Licensed Data, each party shall (i) comply at all times with all Data Protection Laws at its own expense, (ii) employ industry-standard technical and organizational security measures that are appropriate to the risks associated with the use, storage, and maintenance of such data, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, presented by the processing, and (iii) as required by Data Protection Laws, each party shall supply the other party with reasonable cooperation and assistance in connection with any complaint or request in relation to data subject rights and its compliance with Data Protection Laws, in each case arising out of or in connection with the transfer of Client Personal Data or Licensed Data, as the case may be, provided that neither party shall be required to incur material costs or expenses in providing such cooperation and assistance.

(b) With respect to Licensed Data, BrightTALK represents and warrants that: it has satisfied a statutory ground under Data Protection Laws permitting it to transfer Licensed Data to Client in connection with the purposes set forth and described in the Agreement and the applicable Order Form and it has not received any request, notice or other communication from any regulatory body restricting its use of Licensed Data in the manner envisaged by the Agreement and applicable Order Form.

(c) With respect to Client Personal Data, Client represents and warrants that: (i) it has satisfied a statutory ground under Data Protection Laws permitting it to transfer Client Personal Data to BrightTALK in connection with the purposes set forth and described in the Agreement and the applicable Order Form and (ii) it has not received any request, notice or other communication

from any regulatory body restricting its use of Client Personal Data in the manner envisaged by the Agreement and applicable Order Form.

(d) The California Addendum attached to this DPA as Exhibit C applies only where, and to the extent that, the CCPA applies to the processing of Client Personal Data and Licensed Data in the course of providing the Services to Client pursuant to the Agreement.

### 4. Confidentiality.

BrightTALK will maintain all Client Personal Data in strict confidence and will not disclose Client Personal Data to any of its personnel except such personnel as are necessary to perform the Services. BrightTALK will ensure that personnel authorized to process Client Personal Data: (i) have been trained on privacy, confidentiality and security requirements and their responsibilities; (ii) are subject to appropriate contractual and policy obligations regarding confidentiality with language no less restrictive than the obligations provided for under the Agreement or are otherwise under an appropriate statutory obligation of confidentiality; and (iii) do not process Client Personal Data except in accordance with the terms of this DPA and the Agreement, unless otherwise required by Data Protection Laws.

### 5. Sub-Processors.

(a) BrightTALK may engage sub-processors to process Client Personal Data, including those sub-processors currently engaged by BrightTALK as of the Order Form Start Date unless Client provides reasonable written objections in accordance with the terms of Section 5(b) and provided that BrightTALK: (i) will maintain an up-to-date list of its sub-processors at https://www.techtarget.com/terms-and-conditions/ (or successor URL); (ii) will ensure that it has a written agreement in place with its sub-processors that contains data protection obligations no less protective and materially similar than those in this DPA, including providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of Data Protection Laws, where applicable; (iii) will conduct reasonable due diligence on all sub-processors' privacy, security, and compliance programs to ensure that each sub-processor has the capacity to comply with Data Protection Laws and all applicable terms and conditions of this DPA; and (iv) is liable and accountable to Client for its own actions and omissions and those of its sub-processors.

(b) With respect to Client Personal Data, BrightTALK shall notify Client or provide a means for Client to be notified at least thirty (30) days in advance of any new appointment or replacement of a sub-processor. Client may object to BrightTALK's new appointment or replacement of a sub-processor, provided that such objection is in writing and based on reasonable objections relating to the protection of Client Personal Data processed in connection with the Processing Services by such sub-processor within thirty (30) calendar days after receipt of BrightTALK's notice of the use of such new sub-processor. Failure to object to such new sub-processor in writing within the requisite time period shall be deemed as acceptance of the new sub-processor by Client. Client acknowledges and understands that its objection to the use of a sub-processor may prevent Client from using certain Services and/or features thereof. In the event that Client reasonably objects to the use of the new or replacement sub-processor which is necessary to provide the Services, the Parties will work together in good faith to determine whether there is a commercially reasonable alternative method for providing the Services, during which time, BrightTALK shall have the right to cure the objection through one of the following options: (i) BrightTALK shall cease to use the sub-processor with regard to the processing of Client Personal Data; (ii) BrightTALK shall require and ensure that such sub-processor shall take the corrective steps curing the gaps listed by Client in its written objection (which steps will be deemed to resolve Client's objection); or (iii) BrightTALK may cease to provide, temporarily or permanently, the particular Service or feature that would involve use of the sub-processor to process Client Personal Data. If there is no such acceptable commercially reasonable alternative method for providing the Services other than to use the sub-processor in question, Client may reallocate the funds dedicated to such Services to different BrightTALK Services for which the specific sub-processor's services are not required or cancel the Service that would require appointment of the specific sub-processor, subject to payment of any applicable cancellation fees set forth in the Agreement.

(c) Client's sole recourse for its objection to the use of a sub-processor which provides services that are used in connection with optional, value-added, free, third party, or complementary features, integrations, or widgets, shall be to cease using such optional, value-added, free, third party, or complementary features.

### 6. Technical and Organizational Measures.

(a) In addition to maintaining industry-standard technical and organizational security measures that are appropriate to the risks contemplated by the Processing Services, BrightTALK will, at a minimum, maintain technical and organizational measures which are no less protective than the measures set forth in Annex II to Exhibit A. BrightTALK will regularly test, assess, and evaluate the effectiveness of these security measures, no less than once each calendar year. BrightTALK shall

maintain security incident management policies and procedures and in respect of Client Personal Data and, to the extent required under Data Protection Laws, BrightTALK will notify Client without undue delay, and within the timeframes required by Data Protection Laws, upon BrightTALK or any applicable sub-processor becoming aware of any personal data breach affecting Client Personal Data, providing Client with sufficient information to meet obligations to report or inform data subjects of the personal data breach under Data Protection Laws.

(b) With regards to the processing of Client Personal Data, Client shall have the right to assess BrightTALK's compliance with the provisions of this Agreement and, in particular, the implementation of and compliance with appropriate technical and organizational measures. For this purpose, Client may, for example, request from BrightTALK relevant information, existing certificates or audit reports or have BrightTALK's technical and organizational measures inspected by Client or by a competent third party during normal business hours, provided the third party is not in a competitive relationship with BrightTALK. Client shall carry out inspection only to the extent required by Data Protection Laws and shall take into account BrightTALK's business operations. The parties shall in advance agree on the time, manner, and scope of such inspection, as well as any costs to be incurred thereunder.

(c) With regard to the processing of Client Personal Data and at Client's sole expense, Client may submit a reasonable security questionnaire, taking into consideration the type of data processed, to BrightTALK no more than once per calendar year in order to document compliance with the processing obligations outlined in this DPA and performed in connection with Services purchased in the twelve (12) month period leading up to the date of the security questionnaire ("Processing Obligations"). In the event that BrightTALK's responses to said security questionnaire and any reasonable follow-up requests for additional information do not adequately demonstrate BrightTALK's compliance with its Processing Obligations under this DPA, then Client or its appointed third party auditors (subject to reasonable confidentiality obligations) may, upon written request at least thirty (30) days in advance of the proposed audit date and at Client sole expense, conduct a documentary audit of BrightTALK's compliance with its Processing Obligations. To request an audit, Client must submit a detailed proposed audit plan to BrightTALK at least thirty (30) days in advance of the proposed audit date. The proposed audit plan must describe the proposed scope, duration, and start date of the audit. BrightTALK will review the proposed audit plan and communicate any concerns or questions within five (5) business days of receipt. BrightTALK will cooperate with Client to agree on a final audit plan and subject to all applicable confidentiality obligations agreed to by Client and BrightTALK. BrightTALK shall make available to Client any relevant information to demonstrate BrightTALK's compliance with its Processing Obligations ("Compliance Documentation"). Such documentary audit shall take place at an agreed upon location and/or BrightTALK's principal place of business, no more than once per calendar year, unless otherwise required by Data Protection Laws, and during BrightTALK's standard business hours. In the event that Client chooses to utilize the services of a third party representative in connection with this Section 5(c), (i) the third party must be mutually agreed by the Parties in writing prior to commencing such audit, (ii) the third party must be bound by confidentiality obligations and shall apply the same degree of care that it uses to protect its own confidential and proprietary information with respect to any information, documents, and data provided or otherwise made available in connection with the audit including any notes, summaries, reports, or results stemming from such audit, (c) the third party cannot be paid on a contingency basis; and (d) a copy of any audit reports or summaries must be provided to BrightTALK in writing upon completion. The costs associated with the parties' obligations under this Section shall be borne by the respective Parties. If required by law, Client may disclose the results of such security questionnaires and documentary audits or Compliance Documentation to third parties, including competent Data Protection Authorities acting within the scope of their powers and/or law enforcement authority, with the prior written notice to BrightTALK, unless otherwise prohibited by law.

## 7. International Data Transfers.

(a) To the extent that Client's use of the Services requires a transfer of Client Personal Data or Licensed Data outside the EEA, the United Kingdom (the "UK"), or Switzerland the parties will take such measures as are necessary to ensure the transfer is in compliance with applicable Data Protection Laws including the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework as set forth by the U.S. Department of Commerce.

(b) In the event of a transfer of Client Personal Data or Licensed Data subject to the GDPR from the EEA to countries outside the EEA that are not recognized by the European Commission as providing an adequate level of protection for personal data, BrightTALK has adopted and hereby incorporates by reference the EU Standard Contractual Clauses approved by the European Commission to ensure compliance with the requirements of GDPR for international transfers ("EU SCCs"), which are attached to this DPA as Exhibit A.

(c) In the event of a transfer of Client Personal Data or Licensed Data subject to the UK GDPR from the UK to countries outside the UK which is not based on adequacy regulations pursuant to Section 17A of the United Kingdom Data Protection Act 2018 (an "UK Transfer"), the EU SCCs, as amended by the UK Addendum set forth in Exhibit B hereto (as amended, the "UK SCCs") shall apply, and such UK SCCs are deemed entered into and incorporated into this DPA by reference.

(d) In the event of a transfer of Client Personal Data or Licensed Data subject to the Swiss Federal Act of 19 June 1992 on Data Protection ("FADP") and the revised version of the FADP of 25 September 2020 ("Revised FADP") upon its effective date, to countries outside of Switzerland, the Parties agree that all such transfers shall be governed by the EU SCCs subject to the modifications and amendments prescribed by the Swiss Federal Data Protection and Information Commissioner ("FDPIC"). For the sake of clarity, the term "EU Member State'' as used in the EU SCCs shall not be interpreted to exclude data subjects in Switzerland from pursuing their rights in Switzerland in accordance with clause 18(c) and the FDPIC shall act as the "competent supervisory authority" with respect to the transfer of Client Personal Data or Licensed Data comprising Swiss data subjects.

### 8. Data Deletion.

BrightTALK will securely delete all copies of Client Personal Data, within six (6) months of the termination or expiration of the Agreement or sooner if requested by Client in writing, unless otherwise required by applicable law, in which case BrightTALK will immediately inform Client in writing of such requirement. Upon Client's written request, BrightTALK will provide a certificate of deletion within thirty (30) days of such request, certifying that BrightTALK has deleted all personal data. This Section 8 does not apply to data that may be kept during the normal course of business in email or back-up systems. Notwithstanding the foregoing, Client acknowledges and understands that the premature request to delete Client Personal Data may result in the inability to provide Services, impact the performance of Services, or the receipt of deliverables. BrightTALK shall not be held liable for any performance impact, delays, suspensions, or the inability to satisfy quoted performance or deliverables guarantees in the event that Client requests the premature deletion of Client Personal Data.

### 9. Data Protection Impact Assessments, Data Subject Rights and Prior Consultation with Supervisory Authorities.

Upon Client's written request with regard to Client Personal Data, BrightTALK will provide Client with reasonable assistance to complete data protection impact assessments related to the processing activities in connection with this DPA and assistance needed to fulfil Client's obligations under Data Protection Laws, such as the assistance with appropriate technical and organizational measures for the fulfilment of Client's obligation to respond to requests for exercising data subject's rights to the extent Client does not otherwise have access to the relevant information. BrightTALK shall provide, at Client's sole cost, reasonable assistance to Client in the cooperation or prior consultation with a Supervisory Authority relating to BrightTALK's processing of Client Personal Data in connection with this DPA as required by Data Protection Laws.

### 10. Limitation of Liability.

Each Party and each of their Affiliates' liability, taken in aggregate, arising out of or related to this DPA and the EU SCCs and/or UK SCCs, where applicable, whether in contract, tort or under any other theory of liability, will be subject to the limitations and exclusions of liability set out in the "Limitation of Liability" section of the Agreement and any reference in such section to the liability of a party means aggregate liability of that party and all of its Affiliates under the Agreement (including this DPA).

### 11. Government Requests.

(a) BrightTALK undertakes to adopt appropriate technical and organizational measures to protect Client Personal Data in accordance with the requirements of the EU GDPR and UK GDPR (as applicable), including by implementing appropriate technical and organizational safeguards as set out in Annex II of Exhibit A of this DPA to protect Client Personal Data against any interference by a government authority that goes beyond what is necessary in a democratic society to safeguard national security, defense, and public security.

(b) In the event that a government authority submits a request for Client Personal Data, where legally permitted, BrightTALK will notify Client in writing without undue delay and redirect the government entity to request that information directly from Client.

(c) BrightTALK certifies that it has not created (nor knowingly allowed to be created) back doors or similar programming that could be used to access Client Personal Data processed under this DPA on its systems by a government authority or created or changed its business processes in a manner that facilitates access to Client Personal Data processed under this DPA on its systems by government authorities.

### 12. Miscellaneous.

(a) This DPA supersedes and replaces all prior and contemporaneous agreements, oral and written, regarding the processing of the personal data contemplated hereunder. If there is any conflict between this DPA and the Agreement, the terms of this DPA will

control as it relates to the processing of personal data hereunder. If any individual provisions of this DPA are determined to be invalid or unenforceable, the validity and enforceability of the other provisions of this DPA will not be affected.

(b) BrightTALK's obligations under this DPA shall survive expiration or termination of the Agreement and completion of the processing obligations as long as BrightTALK continues to have access to Client Personal Data.

(c) All access to and use of the Services by Authorized Affiliates must comply with the terms and conditions of the Agreement and this DPA and any violation of the terms and conditions therein by an Authorized Affiliate shall be deemed a violation by Client. Client is solely responsible for coordinating all communication with BrightTALK under the Agreement and this DPA and shall be entitled to make and receive any communication in relation to this DPA on behalf of its Authorized Affiliates.

(d) Only a written agreement signed by authorized representatives of both parties can modify this DPA.

(e) This DPA will be governed by and construed in accordance with the governing law and venue set forth in the Agreement.

(f) The Parties hereby consent to the use of any commonly accepted electronic signature system for delivery and acceptance of this DPA and any related documents, and each party agrees that its electronic signature is the same as, and shall have the same force and effect as, a manual signature.

(g) The individuals executing this DPA represent and warrant that they have the right, power, legal capacity and authority to enter into and to execute this DPA on the behalf of their respective legal entities of Client and BrightTALK.

**EXHIBIT A**

# STANDARD CONTRACTUAL CLAUSES

## SECTION I

### Clause 1
*Purpose and scope*

a. The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation)[1] for the transfer of personal data to a third country.
b. The Parties:
   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and
   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

   have agreed to these standard contractual clauses (hereinafter: "Clauses").

c. These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.
d. The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

### Clause 2
*Effect and invariability of the Clauses*

a. These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.
b. These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

### Clause 3
*Third-party beneficiaries*

a. Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:
   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
   ii. Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
   iii. Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
   iv. Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
   v. Clause 13;
   vi. Clause 15.1(c), (d) and (e);
   vii. Clause 16(e);
   viii. Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

b. Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4
*Interpretation*

a. Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.
b. These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.
c. These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5
*Hierarchy*

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6
*Description of the transfer(s)*

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional
*Docking clause*

(*intentionally omitted*)

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8
*Data protection safeguards*

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

**MODULE ONE: Transfer controller to controller (e.g., Module 1 applies where BrightTALK is providing Licensed Data to Client including, among other things, Lead and Demand Generation Services, certain Custom Content Services, certain Platform-related Services and features (e.g., Inbound Converter), List Rental Services, Contact Discovery Services, and Brand Advertising Services).**

**8.1 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

i. where it has obtained the data subject's prior consent;
ii. where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iii. where necessary in order to protect the vital interests of the data subject or of another natural person.

**8.2 Transparency**

a. In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:
    i. of its identity and contact details;
    ii. of the categories of personal data processed;
    iii. of the right to obtain a copy of these Clauses;
    iv. where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.
b. Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.
c. On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.
d. Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.3 Accuracy and data minimisation**

a. Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.
b. If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.
c. The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

**8.4 Storage limitation**

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[2] of the data and all back-ups at the end of the retention period.

**8.5 Security of processing**

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.
b. The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
c. The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.
e. In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.
f. In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.
g. The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

**8.6 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter "sensitive data"), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

**8.7 Onward transfers**

The data importer shall not disclose the personal data to a third party located outside the European Union[3] (in the same country as the data importer or in another third country, hereinafter "onward transfer") unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

i. it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;
iii. the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;
iv. it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;
v. it is necessary in order to protect the vital interests of the data subject or of another natural person; or
vi. where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.8 Processing under the authority of the data importer**

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

**8.9 Documentation and compliance**

a. Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.
b. The data importer shall make such documentation available to the competent supervisory authority on request.

**MODULE TWO: Transfer controller to processor (e.g., Module 2 applies where Client is providing Client Personal Data to BrightTALK including, among other things, for Data Append and Data Cleanse Services, certain features within Platform-related Services (e.g., Opportunity Sync or Fast Pass), and certain Sponsored Content Services).**

**8.1 Instructions**

a. The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.
b. The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

**8.2 Purpose limitation**

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

**8.3 Transparency**

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

**8.4 Accuracy**

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

**8.5 Duration of processing and erasure or return of data**

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the

data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

**8.6 Security of processing**

a. The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.
b. The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.
c. In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.
d. The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

**8.7 Sensitive data**

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

**8.8 Onward transfers**

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[4] (in the same country as the data importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

**8.9 Documentation and compliance**

a. The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b. The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c. The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non- compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.
d. The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.
e. The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9
*Use of sub-processors*

**MODULE TWO: Transfer controller to processor**

a. The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub- processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.
b. Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects.[8] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.
c. The data importer shall provide, at the data exporter's request, a copy of such a sub- processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.
d. The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub- processor to fulfil its obligations under that contract.
e. The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter

shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10
*Data subject rights*

**MODULE ONE: Transfer controller to controller**

a. The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[10] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.
b. In particular, upon request by the data subject the data importer shall, free of charge:
    i. provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);
    ii. rectify inaccurate or incomplete data concerning the data subject;
    iii. erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.
c. Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.
d. The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:
    i. inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and
    ii. implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.
e. Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.
f. The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.
g. If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

**MODULE TWO: Transfer controller to processor**

a. The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.
b. The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex

II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c. In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11
*Redress*

a. The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

**MODULE ONE: Transfer controller to controller**
**MODULE TWO: Transfer controller to processor**

b. In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.
c. Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:
    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
    ii. refer the dispute to the competent courts within the meaning of Clause 18.
d. The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.
e. The data importer shall abide by a decision that is binding under the applicable EU or Member State law.
f. The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12
*Liability*

**MODULE ONE: Transfer controller to controller**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.
c. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
d. The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
e. The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

**MODULE TWO: Transfer controller to processor**

a. Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
b. The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c. Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
d. The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
e. Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
f. The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.
g. The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13
*Supervision*

**MODULE ONE: Transfer controller to controller**
**MODULE TWO: Transfer controller to processor**

a. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

b. The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14
*Local laws and practices affecting compliance with the Clauses*

**MODULE ONE: Transfer controller to controller**
**MODULE TWO: Transfer controller to processor**

a. The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.
b. The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:
    i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c. The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.
d. The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.
e. The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).
f. Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

## Clause 15
*Obligations of the data importer in case of access by public authorities*

**MODULE ONE: Transfer controller to controller**
**MODULE TWO: Transfer controller to processor**

### 15.1 Notification

a. The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:
    i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
    ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.
b. If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.
c. Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).
d. The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e. Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

**15.2 Review of legality and data minimisation**

a. The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).
b. The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.
c. The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

## SECTION IV – FINAL PROVISIONS

### Clause 16
*Non-compliance with the Clauses and termination*

a. The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.
b. In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).
c. The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:
   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
   ii. the data importer is in substantial or persistent breach of these Clauses; or
   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d. Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e. Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the

country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17
*Governing law*

**MODULE ONE: Transfer controller to controller**
**MODULE TWO: Transfer controller to processor**

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18
*Choice of forum and jurisdiction*

**MODULE ONE: Transfer controller to controller**
**MODULE TWO: Transfer controller to processor**

a. Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.
b. The Parties agree that those shall be the courts of Ireland.
c. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.
d. The Parties agree to submit themselves to the jurisdiction of such courts.

## APPENDIX

ANNEX I

### A. LIST OF PARTIES

**MODULE ONE: Transfer controller to controller**

**Data exporter(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: BrightTALK, Inc. and its subsidiaries and affiliates

Address: 275 Grove Street, Newton, MA 02466, USA

Contact person's name, position and contact details: Carmen Picillo, Data Privacy Officer, dpo_ttgt@techtarget.com and Charles D. Rennick, General Counsel, crennick@techtarget.com

Activities relevant to the data transferred under these Clauses:

Transfer of business contact information in connection with Services provided by Exporter.

Signature and date: _____

Role (controller/processor): Controller

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name:

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses: Receipt of business contact information to be used for marketing Importers products and services

Signature and date: _____

Role (controller/processor): Controller

**MODULE TWO: Transfer controller to processor**

**Data exporter(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name:

Address: _____

Contact person's name, position and contact details: _____

_____

Activities relevant to the data transferred under these Clauses:

Transfer of business contact information in connection with Services provided by Importer.

Signature and date: _____

Role (controller/processor): Controller

**Data importer(s):** [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

Name: BrightTALK, Inc. and its subsidiaries and affiliates

Address: 275 Grove Street, Newton, MA 02466, USA

Contact person's name, position and contact details: Carmen Picillo, Data Privacy Officer, dpo_ttgt@techtarget.com and Charles D. Rennick, General Counsel, crennick@techtarget.com

Activities relevant to the data transferred under these Clauses:

Receipt of business contact information to be used for Exporters sales and marketing purposes

Signature and date: _____

Role (controller/processor): Processor

**B. DESCRIPTION OF TRANSFER**

***Categories of data subjects whose personal data is transferred***

| **The Personal Data transferred may concern the following categories of data subjects** | **Applicable Modules under the EU Standard Contractual Clauses** | |
|---|---|---|
| | ***Module One: controller to controller*** | ***Module Two: controller to processor*** |
| Client Employees | Yes. | Yes- If (a) Client integrates a Priority Engine subscription with a sales and nurture stream database (e.g., SFDC) and chooses to utilize certain features in connection with their Priority Engine instance and (b) Client communicates with BrightTALK in connection with the Services, including via its helpdesk ticketing system for the Services. |
| Consumers / Licensed Data (as defined in the Agreement) | Yes. | Yes- If Client provides BrightTALK with a suppression list for use in connection with the Services. |
| Client Customers | No | Yes- If (a) Client integrates a Priority Engine subscription with a sales and nurture stream database and chooses to utilize certain features in connection with their Priority Engine instance, (b) if Client provides BrightTALK with a suppression list for use in connection with the Services, or (c) if Client provides BrightTALK with Client Personal Data in connection with the provision of data hygiene or cleansing services. |
| Vendors | No | No |
| Contractors | No | Yes- If Client integrates a Priority Engine subscription with a sales and nurture stream database and chooses to utilize certain features in connection with their Priority Engine instance and Client's contractors are authorized users of the Service |

**MODULE ONE: Transfer controller to controller (e.g., Module 1 applies where BrightTALK is providing Licensed Data to Client including, among other things, Lead and Demand Generation Services, certain Custom Content Services, certain Platform-related Services and features (e.g., Inbound Converter), List Rental Services, Contact Discovery Services, and Brand Advertising Services).**

**MODULE TWO: Transfer controller to processor (e.g., Module 2 applies where Client is providing Client Personal Data to BrightTALK including, among other things, for Data Append and Data Cleanse Services, certain features within Platform-related Services (e.g., Opportunity Sync or Fast Pass), and certain Sponsored Content Services).**

***Categories of Personal Data Transferred***

| **Types of Personal Data transferred may concern the following types of Personal Data** | **Applicable Modules under the EU Standard Contractual Clauses** | |
|---|---|---|
| | ***Module One: controller to controller*** | ***Module Two: controller to processor*** |
| Personal identification (name, date of birth) | Yes | Yes |
| Government issued identification (driver's license, social security number, or other national identity number) | No | No |
| Contact details (email, phone, address) | Yes | Yes |
| Real-time, precise location tracking | No | No |
| Education and training details | No | No |
| Employment records | No | No |
| Family, lifestyle, and social circumstances | No | No |
| Financial, economic, and insurance data, including financial account numbers | No | No |
| Billing and payment information | No | Yes |
| Digital, device and social identifiers or digital profiles | Yes- Digital/device identifiers only if Client uses Platform Services | No |
| Account credentials | Yes- only such accounts in connection with Client's subscription to BrightTALK's Priority Engine Service | No |
| Contents of communications not directed to BrightTALK or Client or its Authorized Affiliate(s) | No | No |
| Any other categories of Personal Data provided by Client or its Affiliate(s) to BrightTALK in connection with the Processing Services (specify where possible): | Yes- Professional information, including title, position, and employer in connection with Licensed Data and Third Party Integrated Content, and social media handles, provided or appended to data subjects' data. | Yes- Professional information, including title, position only if Client chooses to integrate a subscription to Priority Engine with a sales or nurture stream database and to utilize select features in connection with such services |
| Special categories of data (racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, data concerning health, sex life or sexual orientation) | No | No |
| Platform Service Login Credentials | Yes- provided that Client is purchasing Platform services. | No |
| Licensed Data (as defined in the Agreement) | Yes | No |
| Client Personal Data (as defined in the DPA) | No | Yes |
| Other (specify where possible) | Third Party Integrated Content shared by BrightTALK in connection with a Client's subscription to Priority Engine.<br><br>Visitors to Client's website where Client has deployed the feature-specific | No |

| | | |
|---|---|---|
| | tracking technology only if Client chooses to utilize BrightTALK's website trafficking feature in connection with their subscription to Priority Engine.<br><br>Social media profile details and handles provided, made available, or appended to data subjects' data.<br><br>In the event that Client purchases or utilizes Platform services, technical communications services, including dates and times of connecting to a website or service, records of users' use of the relevant websites and other services, including: registrations, details of content with which users interact, votes, questions, downloads, ratings, feedback, topics, communities, and trends. | |

***Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.***

**MODULE ONE:** *N/A*
**MODULE TWO:** *N/A*

***The frequency of the transfer (e.g., whether the data is transferred on a one-off or continuous basis)***

**MODULE ONE:** *Transfers will be made on a continuous basis, for the duration of the Agreement.*
**MODULE TWO:** *Transfers will be made on a continuous basis, for the duration of the Agreement.*

***Nature of the processing***

**MODULE ONE:** *Exporter shall provide Importer with business contact information obtained through the Services The subject matter of the Processing is BrightTALK's provision of the Services and Platform features thereof described in the Agreement and purchased or utilized by Client, its Affiliates, or its Authorized Contractors (as defined in the Agreement).*
**MODULE TWO:** *Exporter shall provide importer with business contact information and other business information to in furtherance of the Services and enabled Platform features as described in the Importer's product descriptions and the Agreement and utilized by Client, its Affiliates, or its Authorized Contractors (as defined in the Agreement).*

***Purpose(s) of the data transfer and further processing***

**MODULE ONE:** *Business contact information will be transferred to Importer for purposes of sales and marketing Importer's products and services*
**MODULE TWO:** *Business contact information and other business information will be transferred to Importer to allow Importer to provide its Services and access to its Platform as described in the Importer's product descriptions and the Agreement.*

***The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period***

**MODULE ONE:** *Personal Data will be Processed and retained for the duration of the Agreement and subject to Section 8 of the DPA.*
**MODULE TWO:** *Personal Data will be Processed and retained for the duration of the Agreement and subject to Section 8 of the DPA.*

***For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing***

The subject matter, nature, and related information of the Processing undertaken by sub-processors will be set forth in BrightTALK's Sub-Processor List available here: https://www.techtarget.com/terms-and-conditions/.

**C. COMPETENT SUPERVISORY AUTHORITY**

Data Protection Commission (DPC) of Ireland. Under the EU SCCs entered by the parties pursuant to the DPA, Module 2 (Transfer Controller to Processor) the supervisory authority will be the competent supervisory authority that has supervision over the Client Affiliate or other relevant data exporter located in the EEA in accordance with Clause 13 of the Standard Contractual Clauses.

ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

**MODULE ONE: Transfer controller to controller**
**MODULE TWO: Transfer controller to processor**

Description of the technical and organizational security measures implemented by BrightTALK.

| | |
|---|---|
| **(A) Control of physical access to premises** | Technical and organizational measures to control physical access to premises and facilities, particularly to identify permitted personnel at entry:<br>☒ Locked doors on all entrances / exits (e.g., electronic locks; physical locks; etc.)<br>☒ Presence of security personnel (e.g., security at the front desk).<br>☒ Access control systems (e.g., biometric security; access card security; etc.)<br>☒ CCTV systems<br>☒ Additional physical security measures to protect IT systems (e.g., partitioned server room; etc.) (*please specify*): Additional swipe system on server room door. |
| **(B) Control of access to IT systems** | Technical and organizational security measures designed to ensure that users with access to the relevant IT systems are identified and authenticated:<br>☒ IT security systems requiring individual users to log in using unique user names<br>☒ IT security systems requiring the use of strong / complex passwords<br>☒ IT security systems requiring the use of multi-factor authentication<br>☒ Additional system log-in requirements for particular applications<br>☒ Mandatory password changes at fixed intervals (e.g., every 6 months)<br>☒ State-of-the art encryption applied to all data 'in transit'<br>☒ State-of-the art encryption applied to all data 'at rest'<br>☒ Password databases are subject to strong encryption / hashing<br>☒ Regular audits of security procedures<br>☒ Training for employees regarding access to IT systems |
| **(C) Control of access to personal data** | Technical and organizational security measures designed to ensure that users with access to the relevant personal data are identified and authenticated:<br>☒ 'Read' rights for systems containing personal data restricted to specified personnel roles<br>☒ 'Edit' rights for systems containing personal data restricted to specified personnel roles or profiles<br>☒ Logging of all attempts to access systems containing personal data (e.g., recording IP addresses and attempted password and username combinations)<br>☒ State-of-the art encryption on drives and media containing personal data (e.g., using Sophos SafeGuard; TrueCrypt; etc.)<br>☒ Training for employees regarding access to personal data |

| | |
|---|---|
| **(D) Control of disclosure of personal data** | Technical and organizational measures to securely transfer, transmit and communicate or store data on data media and for subsequent checking:<br>☒ Secure data networks (e.g., encrypted VPNs)<br>☒ SSL encryption for all internet access portals<br>☒ Enforced encryption of all drives that are used to take data off the network |
| **(E) Control of input mechanisms** | Technical and organizational security measures to permit the recording and later analysis of information about when input to data systems (e.g., editing, adding, deleting, etc.) occurred and who was responsible for such input:<br>☒ Logging of all input actions in systems containing personal data<br>☒ 'Edit' rights for systems containing personal data restricted to specified personnel roles Profiles<br>☒ Logging of all failed attempts to edit personal data |
| **(F) Control of workflows between controllers and processors** | Technical and organizational measures to segregate the responsibilities between controllers and processors processing the relevant personal data:<br>☒ Binding agreements in writing governing the appointment and responsibilities of processors with access to the relevant personal data<br>☒ Training for employees regarding processing of personal data |
| **(G) Control mechanisms to ensure availability of the relevant personal data** | Technical and organizational measures to ensure the physical and electronic availability and accessibility of the relevant personal data:<br>☒ Documented disaster recovery procedures<br>☒ Secure backup procedures in place, with full backups run regularly<br>☒ Multiple backup facilities and locations<br>☒ Uninterruptible power supplies at backup facilities<br>☒ Physical security of backup facilities (e.g., secure premises; security personnel).<br>☒ Security alarm systems at backup facilities<br>☒ Electronic security of backup facilities (e.g., firewalls; antivirus software; etc.)<br>☒ Environmental controls at backup facilities (e.g., cooling; humidity controls; etc.)<br>☒ Fire protection at backup facilities (e.g., sprinkler systems; fireproof doors; etc.)<br>☒ Secure anonymisation or deletion of personal data that are no longer required for lawful processing purposes<br>☒ Training for employees regarding backups and disaster recovery |
| **(H) Control mechanisms to ensure separation of the relevant personal data from other data** | Technical and organizational measures to ensure that the relevant personal data are stored and processed separately from other data:<br>☒ Logical separation of live or production data from backup data and development or test data<br>☒ Logical separation of drives containing relevant personal data from systems containing other data<br>☒ Separation of personnel processing the relevant personal data from other personnel<br>☒ Training for employees regarding data separation |

**EXHIBIT B**

**UK Addendum**

**International Data Transfer Addendum to the EU Commission Standard Contractual Clauses**

**Part 1: Tables**

Table 1: Parties

| | | |
|---|---|---|
| Start Date | This UK Addendum shall have the same effective date as the DPA | |
| Parties, Details and Key Contact | *See* Annex I to Exhibit A of this DPA | *See* Annex I to Exhibit A of this DPA |

Table 2: Selected SCCs, Modules and Selected Clauses

| | |
|---|---|
| EU SCCs | The EU SCCs which this UK Addendum is appended to as defined in the DPA and completed pursuant to Exhibit A of this DPA. |

Table 3: Appendix Information

"Appendix Information" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs, and for which this UK Addendum is set out in:

| | |
|---|---|
| Annex 1A: List of Parties | As per Table 1 above |
| Annex 1B: Description of Transfer | *See* Annex I to Exhibit A of this DPA |
| Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: | *See* Annex II to Exhibit A of this DPA |
| Annex III: List of Sub processors | *See* Section 5 of the DPA |

**Table 4: Ending this UK Addendum when the Approved UK Addendum Changes**

| | |
|---|---|
| Ending this UK Addendum when the Approved UK Addendum changes | ☒ Importer<br>☒ Exporter<br>☐ Neither Party |

**Entering into this UK Addendum:**

1. *Each party agrees to be bound by the terms and conditions set out in this UK Addendum, in exchange for the other party also agreeing to be bound by this UK Addendum.*

2. *Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making UK Transfers, the Parties may enter into this UK Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this UK Addendum. Entering into this UK Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.*

**Interpretation of this UK Addendum**

3. *Where this UK Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:*

| | |
|---|---|
| UK Addendum | means this International Data Transfer Addendum incorporating the EU SCCs, attached to the DPA as Exhibit A. |
| EU SCCs | means the version(s) of the Approved EU SCCs which this UK Addendum is appended to, as set out in Table 2, including the Appendix Information |
| Appendix Information | shall be as set out in Table 3 |
| Appropriate Safeguards | means the standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a UK transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR. |
| Approved UK Addendum | means the template addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as may be revised under Section 18 of the UK Addendum. |
| Approved EU SCCs | means the standard contractual clauses approved by the European Commission in Commission Decision 2021/914 dated 4 June 2021, for transfers of personal data to countries not otherwise recognized as offering an adequate level of protection for personal data by the European Commission (as amended and updated from time to time). |
| ICO | means the Information Commissioner of the United Kingdom. |
| UK Transfer | shall have the same definition as set forth in the DPA. |
| UK | means the United Kingdom of Great Britain and Northern Ireland |
| UK Data Protection Laws | means all laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018. |
| UK GDPR | shall have the definition set forth in the DPA. |

4. *The UK Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.*

5. *If the provisions included in the UK Addendum amend the Approved EU SCCs in any way which is not permitted under the Approved EU SCCs or the Approved UK Addendum, such amendment(s) will not be incorporated in the UK Addendum and the equivalent provision of the Approved EU SCCs will take their place.*

6. *If there is any inconsistency or conflict between UK Data Protection Laws and the UK Addendum, UK Data Protection Laws applies.*

7. *If the meaning of the UK Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.*

8. *Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or specific provision) has been consolidated, re-enacted and/or replaced after the UK Addendum has been entered into.*

**Hierarchy**

9. *Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for UK Transfers, the hierarchy in Section 10 below will prevail.*

10. *Where there is any inconsistency or conflict between the Approved UK Addendum and the EU SCCs (as applicable), the Approved UK Addendum overrides the EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved UK Addendum.*

11. *Where this UK Addendum incorporates EU SCCs which have been entered into to protect ex-EU Transfers subject to the GDPR, then the parties acknowledge that nothing in the UK Addendum impacts those EU SCCs.*

**Incorporation and Changes to the EU SCCs:**

12. *This UK Addendum incorporates the EU SCCs which are amended to the extent necessary so that:*

    a) together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

    b) Sections 9 to 11 above override Clause 5 (Hierarchy) of the EU SCCs; and

    c) the UK Addendum (including the EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales

13. *Unless the parties have agreed alternative amendments which meet the requirements of Section 12 of this UK Addendum, the provisions of Section 15 of this UK Addendum will apply.*

14. *No amendments to the Approved EU SCCs other than to meet the requirements of Section 12 of this UK Addendum may be made.*

15. *The following amendments to the EU SCCs (for the purpose of Section 12 of this UK Addendum) are made:*

    a) References to the "Clauses" means this UK Addendum, incorporating the EU SCCs;

    b) In Clause 2, delete the words: "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679",

    c) Clause 6 (Description of the transfer(s)) is replaced with: "The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

    d) Clause 8.7(i) of Module 1 is replaced with: "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e) Clause 8.8(i) of Modules 2 and 3 is replaced with: "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f) References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation)" and

"that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g) References to Regulation (EU) 2018/1725 are removed;

h) References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i) The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j) Clause 13(a) and Part C of Annex I are not used;

k) The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l) In Clause 16(e), subsection (i) is replaced with: "the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m) Clause 17 is replaced with: "These Clauses are governed by the laws of England and Wales.";

n) Clause 18 is replaced with: "Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The parties agree to submit themselves to the jurisdiction of such courts."; and

o) The footnotes to the Approved EU SCCs do not form part of the UK Addendum, except for footnotes 8, 9, 10 and 11.

**Amendments to the UK Addendum**

16. *The parties may agree to change Clauses 17 and/or 18 of the EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.*

17. *If the parties wish to change the format of the information included in Part 1: Tables of the Approved UK Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.*

18. *From time to time, the ICO may issue a revised Approved UK Addendum which:*

    a) makes reasonable and proportionate changes to the Approved UK Addendum, including correcting errors in the Approved UK Addendum; and/or

    b) reflects changes to UK Data Protection Laws;

    The revised Approved UK Addendum will specify the start date from which the changes to the Approved UK Addendum are effective and whether the parties need to review this UK Addendum including the Appendix Information. This UK Addendum is automatically amended as set out in the revised Approved UK Addendum from the start date specified.

19. *If the ICO issues a revised Approved UK Addendum under Section 18 of this UK Addendum, if a party will as a direct result of the changes in the Approved UK Addendum have a substantial, disproportionate and demonstrable increase in:*

    a) its direct costs of performing its obligations under the UK Addendum; and/or

b) its risk under the UK Addendum,

*and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that party may end this UK Addendum at the end of a reasonable notice period, by providing written notice for that period to the other party before the start date of the revised Approved UK Addendum.*

20. *The parties do not need the consent of any third party to make changes to this UK Addendum, but any changes must be made in accordance with its terms.*

**EXHIBIT C**

## California Addendum

**Capitalized terms used in this California Addendum that are not otherwise defined in the DPA shall, unless the context clearly provides otherwise, have the same meaning assigned to them in the CCPA.**

A. For instances in which BrightTALK may be deemed a Business, the following provisions shall apply:

1. BrightTALK is providing and Client is using the Licensed Data for its internal business purposes or its business to business sales and marketing efforts as provided in the Agreement, the DPA and this California Addendum.

2. Client will comply with the applicable sections of the CCPA and this California Addendum with respect to the Licensed Data including without limitation, (i) complying with a consumer's request to opt-out of sale or sharing when notified by the consumer or by BrightTALK, (ii) implementing reasonable security procedures and practices appropriate to the nature of the personal information received from BrightTALK and comprising the Licensed Data from unauthorized or illegal access, destruction, use, modification, or disclosure, and (iii) providing the same level of privacy protection as required by the CCPA.

3. Client will notify BrightTALK within the time periods prescribed in the CCPA if it makes a determination that it can no longer meet its obligations under the CCPA. BrightTALK reserves the right to take reasonable and appropriate steps to ensure that Client's use of the Licensed Data is consistent with BrightTALK's obligations under the CCPA, the Agreement, and this California Addendum. Upon notice, BrightTALK may take reasonable and appropriate steps to stop and remediate unauthorized use of the Licensed Data (e.g., BrightTALK may require Client to provide documentation that verifies that Client no longer retains or uses the Licensed Data of consumers who have had their request to opt-out of sale/sharing forwarded to them by BrightTALK). Client shall, where applicable, comply with a consumer's opt-out preference signal.

4. BrightTALK shall notify Client of any consumer request made pursuant to the CCPA that Client must comply with and agrees to provide all information necessary for Client to comply with the request in the periods prescribed under the CCPA. Client agrees to use commercially reasonable efforts to assist BrightTALK except where and to the extent permitted to retain the Licensed Data pursuant to an exemption under the CCPA.

B. For instances in which BrightTALK may be deemed a Service Provider, the following provisions shall apply:

1. Client hereby appoints BrightTALK to process Client Personal Data as provided in the Agreement and consistent with the purchased Services. BrightTALK shall remain responsible for complying with its obligations as a Service Provider and Client shall remain responsible for compliance with its own obligations as a Business. Client shall ensure that it has all necessary rights, permissions, and authorizations under the CCPA for BrightTALK to process the Client Personal Data.

2. BrightTALK agrees to process Client Personal Data for the limited and specified purposes of providing business to business online media and marketing services to Client in accordance with the Agreement, the DPA and this California Addendum as well as Client's selections and use of the Services and as otherwise necessary to provide the Services. BrightTALK will not process Client Personal Data for any other purpose, except where permitted by the CCPA.

3. BrightTALK agrees that it will not: (a) sell or share Client Personal Data; (b) retain, use, or disclose the Client Personal Data for (i) any purpose other than as specified in section 2 above, (ii) any commercial purpose other than providing its Services as specified in the Agreement, (iii) combine the Client Personal Data with other personal information except as permitted under the CCPA; or (iv) any purpose outside of the direct business relationship between BrightTALK and Client.

4. BrightTALK will comply with the applicable sections of the CCPA and this California Addendum and will implement reasonable security procedures and practices appropriate to the nature of the personal information received from the Client and comprising the Client Personal Data from unauthorized or illegal access, destruction, use, modification, or disclosure.

5. Client acknowledges that BrightTALK may engage service providers pursuant to a written contract to assist in processing of the Client Personal Data, in accordance with section 4 of the DPA.

6. BrightTALK will notify Client within the time periods prescribed in the CCPA if it makes a determination that it can no longer meet its obligations under the CCPA. Client reserves the right to take reasonable and appropriate steps to ensure that BrightTALK's use of the Client Personal Data is done in a manner consistent with Client's obligations under the CCPA, the Agreement, and this California Addendum. Upon notice, Client may take reasonable and appropriate steps to stop and remediate unauthorized use of the Client Personal Data (e.g., Client may require BrightTALK to provide documentation that verifies that BrightTALK no longer retains or uses the Client Personal Data of consumers who have had their request to opt-out of sale/sharing forwarded to them by Client).

7. Client shall notify BrightTALK of any consumer request made pursuant to the CCPA that BrightTALK must comply with and agrees to provide all information necessary for BrightTALK to comply with the request in the periods prescribed under the CCPA. BrightTALK agrees to use commercially reasonable efforts to assist Client and shall instruct any subprocessors it has appointed to do the same except where and to the extent permitted to retain the Client Personal Data pursuant to an exemption under the CCPA.