This Data Processing Addendum ("**DPA**"), including its annexes and the corresponding data sheets set forth in **Annex B** ("**Data Sheets**"), is incorporated into the General Terms and Conditions or other master agreement between Customer and DemandTec governing the use of Services (as defined below) by Customer (the "**Agreement**"), and apply to the Processing of Customer Personal Data by DemandTec, on behalf of Customer or Customer's Affiliate(s), in compliance with Data Protection Laws (as defined below).

1. DEFINITIONS

1.1 Unless otherwise set out below, capitalized terms used but not defined in this DPA shall have the same meaning as set forth in applicable Data Protection Laws, the Agreement or the applicable Data Sheet. In this DPA, unless the context requires otherwise:

"**Affiliate(s)**" means any entity that is controlled by or under common control with Customer and who is a beneficiary of the Services under the Agreement.

"**Anonymized Data**" means information that cannot identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual or household.

"**Australian Privacy Act**" means Australia's Privacy Act 1988 (Cth).

"**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code §§ 1798.100 et seq., and any amendments or implementing regulations thereto that are or become effective on or after the effective date of this DPA, including the California Privacy Rights Act ("**CPRA**").

"CDPA" means Virginia's Consumer Data Protection Act 2021.

"CPA" means the Colorado Privacy Act 2021.

"**Controller**" means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information.

"**Controller to Processor SCC"** means the Controller to Processor version of the EU SCC located at https://demandtec.com/contract-terms.

"**Customer Personal Data**" means any information relating to a Data Subject that DemandTec Processes on behalf of the Customer and/or the Customer's Affiliate(s) in connection with DemandTec's provision of Services, including any Personal Information.

"**Data Protection Laws**" means any applicable Law intended to protect the privacy rights of natural persons with regard to the Processing of Customer Personal Data, these may include (without limitation) the GDPR, the UK GDPR, the CCPA, the CPRA, the CPA, the CDPA, the Australian Privacy Act, the Indian Privacy Laws, the PDPA and the LGPD.

"**Data Subject**" means an identified or identifiable natural person to whom the data relates.

“EU SCC” means the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council and the European Commission’s Implementing Decision (EU) 2021/914 of 4 June 2021.

"**GDPR**" means the EU General Data Protection Regulation 2016/679 of the European Parliament and of the Council and any national Law of the European Economic Area member states ("**EEA**") implementing or supplementing this regulation, in each case as amended, replaced or superseded from time to time, and all applicable Laws of the European Union or the EEA member states privacy rights with regard to the Processing of Personal Information.

“**LGPD**” means the Brazilian General Data Protection Law, No. 13,709/2018.

"**Indian Privacy Laws**" means the Information Technology Act, 2000 and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

"**PDPA**" means the Personal Data Protection Act of Singapore.

"**Personal Information**" means any information within the scope of the definition of that term under the CCPA, any information within the scope of "personal data" as such term is defined in the GDPR, and any information within the scope of another reasonably equivalent term under another applicable Data Protection Law.

"**Processing**" means any operation or set of operations that is performed on Personal Information, or on sets of Personal Information, whether or not by automated means as defined under the GDPR, and "**Process**" and “**Processes**” will be interpreted accordingly.

"**Processor**" means, as applicable, (a) the entity that Processes Personal Information on behalf of a Controller, (b) the “**data intermediary**” as such term is defined in the PDPA, and (c) the “**service provider**” as such term is defined in the CCPA.

"**Processor to Processor SCC”** means the Processor to Processor version of the EU SCC located at https://demandtec.com/contract-terms.

“**Security Incident**” means any accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, any Customer Personal Data.

"**Services**" means the service(s) provided by DemandTec to Customer pursuant to the Agreement.

“UK GDPR” means the (Retained EU Legislation) Regulation (EU) 2016/679 (United Kingdom General Data Protection Regulation) (UK GDPR) as defined in and supplemented by the United Kingdom’s Data Protection Act 2018.

"UK Addendum" means means the International Data Transfer Addendum to the EU SCC, issued by the United Kingdom's Information Commissioner under S119A(1) Data Protection Act 2018 located at https://demandtec.com/contract-terms.

1.2 This DPA supplements the Agreement with respect to any Processing of Customer Personal Data and replaces all prior agreements regarding this subject matter. In the event of conflict between the DPA and the terms of the Agreement, the terms of the DPA shall prevail. Additional details regarding the Processing under this DPA are set forth in the relevant Data Sheet.

1.3 **Role of the Parties**. Customer and DemandTec agree that:

(a) For purposes of the GDPR and any and all other applicable Data Protection Laws, Customer and/or Customer's Affiliate(s), as applicable, is the Controller of Customer Personal Data, and

DemandTec is the Processor of such data, except when Customer or Customer's Affiliate(s) act as a Processor of Customer Personal Data, in which case DemandTec is a subprocessor. Customer will identify and inform DemandTec of other Controllers, if any, prior to providing their Customer Personal Data in accordance with the Data Sheet.

(b) For purposes of the CCPA, Customer and/or Customer's Affiliate(s), as applicable, is the "business" (as defined in Cal. Civ. Code §1798.140), and DemandTec will act as a "service provider" *(ibid.)* in its performance of its obligations under the Agreement. DemandTec will not retain, use, or disclose any "personal information" (*ibid.*) included in the Customer Personal Data for any purpose other than DemandTec's performance of its obligations under the Agreement, or as otherwise permitted by the CCPA.

1.4 If Customer Personal Data of Customer's Affiliate(s) is Processed, Customer's Affiliate(s) providing such data shall have the same rights and obligations as the Customer under this DPA.

2. SPECIFICATION OF THE DATA PROCESSING

2.1 A list of categories of Data Subjects, types of Customer Personal Data, including information on special categories of Personal Information, subject matter and nature and purpose of Processing is set out in the Data Sheet corresponding with each Service. When DemandTec is providing Professional Services, DemandTec shall take reasonable measures to avoid access to Personal Information, however, the Parties understand and acknowledge that incidental access to Personal Information stored within the Customer's data processing system cannot be excluded when providing such Professional Services. Unless provided for otherwise in the Agreement, the subject matter of the Processing will be in this case providing the Professional Services for the Customer.

2.2 Services are provided on the assumption that their use is limited to the categories of Data Subjects and types of Customer Personal Data, including information on special categories of Personal Information, as described in the Data Sheets. If Customer believes that certain types of Customer Personal Data or Data Subjects are not (or not sufficiently) covered by the corresponding Data Sheet, Customer shall inform DemandTec and seek DemandTec's consent before any such Processing can take place. Such consent

shall not be unreasonably withheld; reasonable bases for withholding consent exist where: (a) the quality of Processing would be degraded or (b) DemandTec would need to modify its technical or organizational security measures to responsibly process such data, for example, if such modification would be required to satisfy legal requirements related to the Processing of such data due to its sensitivity. Any use of the Services in deviation of what has been agreed to in the Data Sheets constitutes a breach of contract and is the sole responsibility of the Customer.

2.3 In addition to the subject matter, nature and purpose of the Processing as set out in the corresponding Data Sheet, the Parties agree that anonymizing the Customer Personal Data is an additional subject matter of the Processing.

2.4 The duration of the Processing corresponds to the duration of the Services, unless otherwise stated in the Data Sheet.

3. INSTRUCTIONS AND COMMUNICATION BETWEEN THE PARTIES

3.1 Unless otherwise required by applicable Law, DemandTec will Process Customer Personal Data according to Customer's instructions which are embodied in the Agreement, DemandTec Documentation and Customer's and Customer's Authorized Users' use and configuration of the Services. Such instructions may include transfers of Customer Personal Data to a country not providing an adequate level of protection pursuant to the applicable Data Protection Laws ("**Third Country**") or an international organization. If DemandTec is required by applicable Law to Process Customer Personal Information in a manner other than as instructed by Customer and is not prohibited by applicable Law from disclosing such legal requirement, then DemandTec will inform Customer of such legal requirement before engaging in such Processing.

3.2 If DemandTec believes an instruction violates applicable Law, DemandTec will inform Customer without undue delay, and may suspend the performance of such instruction until Customer has modified or confirmed its lawfulness in writing.

3.3 Customer may provide further legally required instructions regarding the Processing of Customer Personal Data ("**Additional Instructions**") as described in Section 11 below. If DemandTec notifies Customer that an Additional Instruction is not feasible, the Parties shall work together to find a reasonable alternative. If DemandTec notifies the Customer that neither the Additional Instructions nor an alternative is feasible, Customer may terminate the affected Service, in accordance with any applicable terms of the Agreement.

3.4 Customer shall serve as the single point of contact for DemandTec in regard to this DPA. As other Controllers may have certain direct rights against DemandTec, Customer undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from such Controllers. DemandTec shall be discharged of its obligation to inform or notify another Controller when DemandTec has provided such information or notice to Customer. Similarly, DemandTec will serve as the single point of contact for Customer with respect to its obligations as a Processor under this DPA. Customer shall provide written notice to DemandTec with the name and contact information of the person designated by Customer to be responsible for dealing with questions relating to applicable Data Protection Laws and data security in the context of performing this DPA.

4. DEMANDTEC'S OBLIGATIONS

4.1 DemandTec will comply with Data Protection Laws applicable to DemandTec in its role as Processor in performing the Services. DemandTec is not responsible for determining the legal requirements applicable to Customer's business, or for determining whether a Service meets any such requirements.

4.2 DemandTec shall ensure that (i) access to Customer Personal Data is limited to personnel performing Services under the Agreement and (ii) such personnel have committed themselves to confidentiality and only process Customer Personal Data in accordance with this DPA, the Agreement, Customer's documented instructions or as required by Law.

4.3 DemandTec will inform Customer of requests DemandTec receives directly from Data Subjects exercising their Data Subject rights regarding Customer Personal Data under applicable Data Protection Laws (*e.g.*, including access to, rectification, deletion and blocking of data). Customer shall be responsible for handling such requests. Subject to Section 11 below, DemandTec will assist Customer in handling such requests.

4.4 DemandTec will assist Customer by providing appropriate technical and organizational measures for the fulfilment of Customer's obligation to respond to Data Subject rights requests under the Data Protection Laws.

4.5 DemandTec shall assist Customer in complying with the obligations pursuant to the Data Protection Laws, including Art. 32 through 36 GDPR (Security of Processing, Data Security Breach Notification, Data Protection Impact Assessment, Consultation with Data Protection Supervisory Authorities).

4.6 DemandTec will implement technical and organizational data-security measures, pursuant to the Data Protection Laws, including Art. 32 GDPR, and in accordance with Section 6 of this DPA.

4.7 For the purpose of enabling Customer to comply with its own notification obligations with regard to Security Incident pursuant to Data Protection Laws, including Art. 33 para 1 and Art. 34 para 1 GDPR, DemandTec shall notify Customer without undue delay and no later than 72 hours after becoming aware of any Security Incident.

4.8 In the case claims based on Art. 82 GDPR are raised against Customer, DemandTec shall reasonably support Customer with its defence to the extent such claims arise in connection with the Processing of Customer Personal Data by DemandTec.

4.9 DemandTec will inform Customer of the name and the official contact details of its data protection officer as required under applicable Laws. The data protection officer may serve as the single point of contact pursuant to Section 3.4 of this DPA.

5. CUSTOMER'S OBLIGATIONS

5.1 Customer is responsible for the lawfulness of the Processing of the Customer Personal Data, including, to the extent required under applicable Data Protection Laws, by ensuring Data Subjects have received adequate notice of, exercised adequate consent with regard to or otherwise adequately authorized the Processing of their Personal Information. Customer is also responsible for complying with Data Subject

requests. Customer will not use the Services in a manner that would violate the rights of any Data Subject or otherwise violate applicable Data Protection Laws.

5.2 In the case claims based on Art. 82 GDPR are raised against DemandTec, Customer shall reasonably support DemandTec with its defence to the extent such claims arise in connection with the Processing of Customer Personal Data by DemandTec.

6. TECHNICAL AND ORGANISATIONAL MEASURES

6.1 DemandTec will implement and maintain the technical and organizational measures ("**TOM**") set forth in the Data Security and Privacy Principles, annexed as **Annex A** to the DPA, or the corresponding Data Sheet, reasonably designed and implemented to provide a level of security appropriate to the risk. In assessing the appropriate level of security, due consideration shall be given to the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data transmitted, stored or otherwise Processed.

6.2 DemandTec reserves the right to modify the TOM provided that the overall functionality and security of the Services are not degraded. Modifications to the TOM must be reasonably designed and implemented to provide an appropriate level of security. DemandTec shall make available to Customer a description of any material modifications to the TOM which enables Customer to assess compliance with the Data Protection Laws, including Art. 32 GDPR. If DemandTec provides notification to Customer of any such material modifications, Customer may object in writing to the proposed modifications within two (2) weeks of their provision by DemandTec. Customer shall only be entitled to object to modifications that are not reasonably designed and implemented to provide an appropriate level of security. If Customer fails to provide timely and valid written objection, such failure shall be deemed consent and any objection waived. In case of timely and valid objection, DemandTec may suspend the affected portion of the Services. Customer shall not be entitled to a pro-rata refund for the suspended portion of the Services unless Customer can demonstrate that the modified TOM are not reasonably designed and implemented to provide an appropriate level of security.

7. SUBPROCESSOR

7.1 DemandTec may engage other Processors to Process Customer Personal Data ("**Subprocessors**").

7.2 Any Subprocessor is obliged, before initiating the Processing, to commit itself in writing for the benefit of Customer and Customer Affiliate(s) to comply with the same data protection obligations as the ones under this DPA.

7.3 The agreement with the Subprocessor must provide at least the level of data protection required by this DPA, including requirements to implement appropriate TOM. Where the Subprocessor fails to fulfil its data protection obligations, DemandTec shall remain fully liable to Customer for the performance of the Sub-processor's obligations.

7.4 By entering into this DPA, Customer authorizes engagement of the Subprocessors identified in the

corresponding Data Sheet. Upon Customer's written request, DemandTec shall provide Customer with relevant information on data protection obligations of Subprocessors, including granting Customer appropriate access to relevant contractual documents.

7.5 DemandTec shall audit its Subprocessors on a regular basis and will, upon Customer's written request, confirm Subprocessor compliance with Data Protection Laws and data processing agreements. Where Customer demonstrates legitimate grounds, Customer may instruct DemandTec in writing to provide additional information regarding Subprocessor data protection compliance, and DemandTec shall undertake reasonable efforts to comply with such requests.

7.6 DemandTec will notify Customer within a reasonable timeframe of any addition to or replacement of the current Subprocessors. Such notice may be provided by email or posting the updated information on a website accessible to Customer.

7.7 Within thirty (30) days after notification of any change in Subprocessors, Customer may object in writing (an **"Objection"**). Any such written objection must include Customer's specific reasons for its objection and proposed options to mitigate alleged risk, if any. In the absence of timely Objection, Subprocessors identified by DemandTec to Customer may be commissioned to Process Customer Personal Data.

7.8 If Customer provides timely Objection to the addition of a Subprocessor and DemandTec cannot reasonably accommodate Customer's proposed options to mitigate alleged risk, DemandTec will notify Customer. Customer may then terminate the affected Services as set out in the Agreement. Such termination shall not relieve Customer of its payment obligations set forth in a Quote.

8. INTERNATIONAL TRANSFERS OF CUSTOMER DATA

8.1 In the case of a transfer of Customer Personal Data to a Third Country, the Parties shall cooperate to ensure compliance with applicable Data Protection Laws as set out in the following Sections. If Customer believes the measures set out below are insufficient to satisfy legal requirements under any particular circumstances, Customer shall provide written notice of its grounds for such opinions to DemandTec and the Parties shall work together to find a mutually agreeable alternative.

8.2 By entering into the Agreement, and provided the Customer and/or another Controller (if Customer is acting on behalf of other Controllers) is/are located in the European Union or the United Kingdom, Customer is entering into EU SCC (where located in the European Union) or UK Addendum (where located in the United Kingdom) with (i) each Subprocessor listed in the Data Sheet that is a DemandTec Affiliate located in a Third Country ("**DemandTec Data Importers**") or (ii) a Subprocessor also in a Third Country that is not a DemandTec Affiliate ("**Third Party Data Importer**"),:

(a) if Customer is located in the European Union and is a Controller of all or part of the Customer Personal Data, Customer is entering into the Controller to Processor SCC in respect to such Customer Personal Data;

(b) if Customer is located in the European Union and is acting as Processor on behalf of other Controllers of all or part of the Customer Personal Data, then Customer is entering into the Processor to Processor SCC provided that Customer has entered into separate EU Standard

Contractual Clauses with the Controllers; and

(c) if Customer is located in the United Kingdom, Customer is entering the UK Addendum

8.3 Subject to the aforementioned Customer's right to object to Subprocessors, Customer gives DemandTec a general authorisation that any new DemandTec Data Importer and/or any new Third Party Data Importer engaged by DemandTec in accordance with this Section 8 shall become an additional data importer under the SCC or UK Addendum (as applicable). Customer herewith authorizes DemandTec to enter into the Processor to Processor SCC or UK Addendum (as applicable) with DemandTec Data Importers in the name of and on behalf of the Customer.

8.4 If Customer is unable to agree to the EU SCC or UK Addendum (as applicable) on behalf of another Controller, as set out in Sections 8.2 and 8.3, Customer will procure the agreement of such other Controller to enter into those agreements directly. Additionally, Customer agrees and, if applicable, procures the agreement of other Controllers that the EU SCC or UK Addendum (as applicable), including any claims arising from them, are subject to the terms set forth in the Agreement, including the exclusions and limitations of liability.

8.5 In case of conflict between the DPA and the EU SCC, the EU SCC shall prevail.

8.6 In case of conflict between the DPA and the UK Addendum, the UK Addendum shall prevail.

9. AUDIT

9.1 In response to Customer's written request and subject to a non-disclosure agreement, DemandTec shall provide to Customer sufficient documentation related to the TOM to demonstrate compliance with this DPA. The effectiveness of DemandTec's TOM may be demonstrated on an annual basis by documentation provided by an independent third-party evaluating the TOM, for example an ISO/IEC 27001 Certificate, an SSAE18 SOC 2 Type II or equivalent attestation report, or similar certification or attestation. DemandTec will reasonably cooperate with Customer where requested, by providing available additional information concerning the TOM, to help Customer better understand such TOM.

9.2 If Customer provides legitimate grounds to allege, or raise serious concerns about, the potential non-compliance of DemandTec's TOM, Customer is, subject to a non-disclosure agreement and no more frequently than once per year (absent specific indicators warranting differently), entitled to audit DemandTec with respect to its TOM compliance.

9.3 This audit right can be exercised by (i) requesting additional information in writing, such as documentation on the processing of Customer Personal Data or (ii) by inspecting DemandTec's working premises where Customer Personal Data is accessible, provided that such inspection shall be conducted in a manner that minimizes the risk of Customer access to data of other customers or to DemandTec's confidential information. Alternatively, Customer may designate an independent, qualified third-party to perform such tasks on its behalf. Any such designated third-party must agree to a non-disclosure agreement, shall not be a direct competitor of DemandTec and must be able to demonstrate industry-recognized credentials and qualifications to conduct such audits.

9.4 The costs associated with such audits and/or for providing additional information shall be borne by Customer, unless factual evidence conclusively demonstrates a material breach of this DPA by DemandTec.

10. RETURN OR DELETION OF CUSTOMER PERSONAL DATA

10.1 Subject to clause 10.2, upon termination or expiration of the Agreement DemandTec will, at the choice of the Customer, either delete or return Customer Personal Data, provided such deletion or return does not conflict with superseding legal obligations.

10.2 The Parties agree that, if the Customer has not made a choice pursuant to Section 10.1 within ten (10) days of termination of the Agreement, Customer will be deemed to have chosen to have the Customer Personal Data deleted by DemandTec and waived any objection to such deletion, unless such deletion would conflict with superseding legal obligations.

11. ADDITIONAL INSTRUCTIONS

If Customer's instructions lead to a change from, or increase of, the agreed Services, or in the case of DemandTec's compliance with its obligations pursuant to this DPA to assist Customer with Customer's own statutory obligations, DemandTec is entitled to charge reasonable fees for such tasks, based on the prices agreed for rendering the Services and/or communicated to Customer in advance.

ANNEX A

DATA SECURITY AND PRIVACY PRINCIPLES

The technical and organizational measures provided in this Data Security and Privacy Principles annex ("**DSP**") apply to DemandTec SaaS Products, including any underlying applications, platforms, and infrastructure components operated and managed by DemandTec in providing the SaaS Product ("**Components**"), except where Customer is responsible for data security and privacy or otherwise specified in writing between DemandTec and Customer. Customer is responsible for: a) determining whether the SaaS Product is suitable for Customer's use and; b) implementing and managing security and privacy measures for elements not provided and managed by DemandTec within the SaaS Product described in applicable attachments ("**Attachments**") to this document, the Data Protection Agreement (DPA) or the Agreement (such as systems and applications built or deployed by Customer, or Customer end-user controls to restrict and protect access to Software as a Service offerings). The measures implemented and maintained by or on behalf of DemandTec within each SaaS Product will be subject to annual certification of compliance by DemandTec with ISO 27001 or SSAE SOC 2 or both.

1. DATA PROTECTION

1.1 Security and privacy measures for each SaaS Product are designed in accordance with DemandTec's secure- engineering and privacy-by-design practices to protect Customer data and files ("**Content**") input into a SaaS Product, and to maintain the availability of such Content pursuant to the Agreement, including applicable Attachments and transaction documents. Customer is the sole Controller for any Personal Data included in the Content and appoints DemandTec as a processor to process such personal data (as those terms are defined in Regulation (EU) 2016/679, General Data Protection Regulation). DemandTec will treat all Content as confidential by not disclosing Content except to DemandTec employees, contractors, and sub- processors, and only to the extent necessary to deliver the SaaS Product, unless otherwise specified in an Attachment.

1.2 DemandTec will verify that physical storage media owned and operated by DemandTec and intended for reuse are securely sanitized prior to such reuse and will verify the destruction of such media not intended for reuse, consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST), guidelines for media sanitization.

1.3 Upon written request, DemandTec will provide reasonable evidence of stated compliance and accreditation, which may, where available, comprise certificates, attestations, or reports resulting from accredited independent third-party audits, such as ISO 27001, SSAE SOC 2, and/or other industry standards as specified in an Attachment. Where applicable, the accredited independent third-party audits will occur at the frequency required by the relevant standard to maintain the SaaS Product's stated compliance and accreditation.

1.4 data security and privacy information specific to a SaaS Product may be available in a relevant Attachment (such as a Data Sheet) or other standard documentation to aid in Customer's initial and ongoing assessment of a SaaS Product's suitability for use. Such information may include evidence of stated certifications and accreditations, information related to such certifications and accreditations, data sheets, FAQs, and other generally available documentation. DemandTec will direct Customer to available

standard documentation if asked to complete Customer-preferred questionnaires or forms, and Customer agrees such documentation will be utilized in lieu of any such request. DemandTec may charge an additional fee to complete any Customer-preferred questionnaires or forms or to provide consultation to Customer for such purposes.

2. SECURITY POLICIES

2.1 DemandTec will maintain and follow information-technology ("**IT**") security policies and practices that are integral to DemandTec's business and mandatory for all DemandTec employees. The Chief Information Security Officer will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

2.2 DemandTec will review its IT security policies at least annually and amend such policies as DemandTec deems reasonable to maintain protection of SaaS Products and Content processed therein.

2.3 DemandTec will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly owned DemandTec subsidiaries. In accordance with DemandTec internal process and procedures, these requirements will be periodically reviewed and may include criminal background checks, proof of identity validation, and additional checks as deemed necessary by DemandTec. Each DemandTec company is responsible for implementing such requirements in its hiring process as applicable and permitted under local Law.

2.4 DemandTec employees will complete security and privacy education annually and certify each year that they will comply with DemandTec's ethical business conduct, confidentiality, and security policies. Additional policy and process training may be provided to persons granted administrative access to SaaS Product Components that is specific to their role within DemandTec's operation and support of the SaaS Product, and as required to maintain compliance and any certifications stated in the relevant Attachment.

3. SECURITY INCIDENTS

3.1 DemandTec will follow documented incident-response policies consistent with NIST guidelines for computer Security Incident handling and will comply with data-breach notification terms of the Agreement.

3.2 DemandTec will investigate unauthorized access to and unauthorized use of Content of which DemandTec becomes aware, and, within the SaaS Product scope, DemandTec will define and execute an appropriate response plan. Customer may notify DemandTec of a suspected vulnerability or incident by submitting a technical support case.

3.3 DemandTec will notify Customer without undue delay upon confirmation of a Security Incident that is known by DemandTec to affect Customer. DemandTec will provide Customer, in response to a reasonable written request, information about such Security Incident and the status of any DemandTec remediation and restoration activities, including, if required by applicable Data Protection Laws, (i) a description of the Security Incident, including the date and time the Security Incident was discovered; (ii) an overview of the affected Personal Information; (iii) the number of affected Data Subjects; (iv) the expected consequences

of the Security Incident; (v) a description of the measures taken by DemandTec to restrict such consequences.

4. PHYSICAL SECURITY AND ENTRY CONTROL

4.1 DemandTec will verify the maintenance of appropriate physical-entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into facilities used to host the SaaS Product ("**Data Centers**"). Auxiliary entry points into Data Centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

4.2 Access to Data Centers and controlled areas within Data Centers will be limited by job role and subject to authorized approval. Use of an access badge to enter a Data Center and controlled areas will be logged, and such logs will be retained for not less than one year. DemandTec will revoke or procure the revocation of access to controlled Data Center areas upon separation of an authorized employee. DemandTec will follow formal documented separation procedures that include prompt removal from access-control lists and surrender of physical access badges.

4.3 DemandTec will ensure, including the securing of relevant contractual commitments from third party vendors, that any person duly granted temporary permission to enter a Data Center facility or a controlled area within a Data Center will be registered upon entering the premises; must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

4.4 DemandTec will verify that the operators of the Data Centers take all necessary and required precautions to protect the SaaS Product's physical infrastructure against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

5. ACCESS, INTERVENTION, TRANSFER AND SEPARATION CONTROL

5.1 Documented security architecture of networks managed by or on behalf of DemandTec in its operation of the SaaS Product will be maintained. Such network architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, will be reviewed for compliance with secure segmentation, isolation, and defense-in-depth standards prior to implementation. SaaS Product networks do not use wireless-networking technology. Wireless-networking technology may be used in the maintenance and support of the SaaS Product and associated Components. Such wireless networks, if any, will be encrypted, will require secure authentication, and will not provide direct access to SaaS Product networks.

5.2 Measures that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons will be maintained for each SaaS Product. Appropriate isolation of its production and non-production environments will be maintained, and, if Content is transferred to a non-production environment, for example in order to reproduce an error at Customer's request, security and privacy

measures designed to provide the same level of protection as in the production environment will be maintained in the non-production environment.

5.3 To the extent described in the relevant DemandTec Documentation, Content not intended for public or unauthenticated viewing will be encrypted when transferred over public networks, and the SaaS Product shall enable use of a cryptographic protocol, such as HTTPS or SFTP, for Customer's secure transfer of Content to and from the SaaS Product over public networks.

5.4 Content will be encrypted at rest when and as specified in the relevant DemandTec Documentation. If the SaaS Product includes management of cryptographic keys, documented procedures will be maintained for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

5.5 If access to Content is required, it will be restricted to the minimum level required. Such access, including administrative access to any underlying Components ("**Privileged Access"**), will be individual, role-based, and subject to approval and regular validation by authorized personnel following the principles of segregation of duties. Adequate measures will be maintained to identify and remove redundant and dormant accounts with Privileged Access and such Privileged Access will promptly be revoked upon the account owner's separation from DemandTec or upon the request of authorized personnel, such as the account owner's manager.

5.6 Consistent with industry standard practices, and to the extent natively supported by each Component managed by or on behalf of DemandTec within the SaaS Product, technical measures will be maintained enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases.

5.7 Use of Privileged Access will be monitored and maintained and security information and event management measures will be maintained and designed to: a) identify unauthorized access and activity; b) facilitate a timely and appropriate response; and c) enable internal and independent third-party audits of compliance with documented policy.

5.8 Logs in which Privileged Access and activity are recorded will be retained in compliance with DemandTec's records-management plan. Measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs will be maintained.

5.9 To the extent supported by native device or operating system functionality, computing protections for its end-user systems will be maintained that include endpoint firewalls, full-disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint-management solutions that enforce security configuration and patching requirements.

6. SERVICE INTEGRITY AND AVAILABILITY CONTROL

6.1 DemandTec will: a) ensure security and privacy risk assessments of its SaaS Products are carried out at least annually; b) ensure penetration testing and vulnerability assessments, including automated system and application security scanning and manual ethical hacking, are carried out before production release

and annually thereafter; c) ensure a qualified independent third-party performs penetration testing at least annually; d) ensure automated management and routine verification of underlying Components' compliance with security-configuration requirements are carried out; and e) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact.

6.2 DemandTec will take reasonable steps to avoid SaaS Product disruption when performing tests, assessments, scans, and execution of remediation activities.

6.3 DemandTec will maintain policies and procedures designed to manage risks associated with the application of changes to its SaaS Products. Prior to implementation, material changes to a SaaS Product, including its systems, networks, and underlying Components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the SaaS Product and its Customers, expected outcome, rollback plan, and documented approval by authorized personnel.

6.4 DemandTec will maintain an inventory of all information-technology assets used in its operation of the SaaS Product. DemandTec will continuously monitor and manage the health, including capacity, and availability of the SaaS Product and underlying Components.

6.5 Each SaaS Product will be separately assessed for business-continuity and disaster-recovery requirements pursuant to documented risk-management guidelines. Each DemandTec SaaS Product will have, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business-continuity and disaster-recovery plans consistent with industry-standard practices. Recovery-point and recovery-time objectives for the SaaS Product, if provided, will be established with consideration given to the SaaS Product's architecture and intended use, and will be described in the relevant Attachment. Customer’s Content on physical media intended for off-site storage, if any, such as media containing SaaS Product backup files, will be encrypted prior to transport.

6.6 DemandTec will maintain measures designed to assess, test, and apply security patches to the SaaS Product and its associated systems, networks, applications, and underlying Components within the SaaS Product scope. Upon determining that a security patch is applicable and appropriate, DemandTec will implement the patch pursuant to documented severity and risk-assessment guidelines. Implementation of security patches will be subject to DemandTec change-management policy.

[END OF ANNEX]

ANNEX B

DATA SHEETS

The relevant Data Sheet(s) can be found here: DemandTec.com/contract-terms.

[END OF ANNEX]