Exhibit
Data Protection terms

1. **Definitions and interpretation**

1.1 Any requirement for writing and any notice to be given by either Party under this Exhibit (Data Protection terms) shall be satisfied by e-mail unless stated otherwise in this Exhibit.

1.2 The terms defined below shall have the meaning defined below, but only for the purposes of this Exhibit (and also for the purposes of the Agreement, if they are specifically referred to in the Agreement):

"**Affiliate**" means an entity that, either directly or indirectly, controls, is controlled by, or is under common control with, the relevant entity, where "control" means the ability to direct the affairs of another by ownership, contract or otherwise.

"**Agreement**" means the Agreement/Purchase Order between Client and Supplier of which this Exhibit is a part.

"**Client**" means the Philip Morris International entity that is a party to the Agreement.

"**Client Data**" means data that either:

(a) the Client, or a person acting on its behalf, provides to the Supplier, or permits the Supplier to access, in connection with this Agreement; or

(b) the Supplier creates in providing the Services.

"**Client Group**" means the Client and all its Affiliates (and "member of the Client Group" shall be construed accordingly).

"**Client Personal Data**" means Client Data that is Personal Data.

"**Data Breach**" means any breach of security leading to the accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of, or access to, Client Personal Data transmitted, stored or otherwise Processed.

"**Data Controller**" means a person who, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means a person who Processes Personal Data on behalf of a Data Controller.

"**Data Protection Law**" means the law protecting the fundamental rights and freedoms of persons and, in particular, their right to privacy, with regard to the Processing of Personal Data.

"**Data Subject**" means an identified or identifiable individual. An "identifiable" individual is one who can be identified, directly or indirectly, including by reference to an identifier, such as a name, identification number location data, an online identifier or to one or more factors specific to his physical, physiological, genetic, mental, economic, cultural or social identity.

"**Exhibit**" means this Exhibit.

"**Permitted Subcontractor**" means a subcontractor that the Client has permitted in accordance with the provisions in the Agreement that govern subcontracting.

"**Personal Data**" means any information relating to a Data Subject.

to "**Process**" (and variants of it, such as "Processing") means to perform any operation or set of operations upon data, whether or not by automatic means, such as collecting, recording, organising, storing, adapting or altering, retrieving, consulting, using, disclosing (by transmission, dissemination or otherwise making available), aligning or combining, blocking, erasing or destroying.

"**Public Holiday**" means a day officially recognised as a holiday in the local administrative area of the Client's registered office.

"**paragraph**" means a paragraph of this Exhibit.

"**Security Event**" shall have the meaning given to that term in paragraph 2.9.

"**Services**" means the services to be provided under the Agreement.

"**Subprocessor**" shall have the meaning given to that term in paragraph 2.3.

"**Supplier**" means the party to the Agreement that is not a member of the Client Group.

"**Working Day**" means a day that is neither a Sunday, a Public Holiday, nor a day that the Client informs the Supplier is, for the purposes of this Agreement, a company holiday for the Client or any member of the Client Group (as appropriate).

2. Rights and obligations of the Supplier and the Client – Supplier as Data Processor of Client Personal Data

2.1 This paragraph 2 applies to all the Supplier's Processing of Client Personal Data, save where the Supplier Processes Client Personal Data as a Data Controller in accordance with paragraph 4.

2.2 Appointment of the Supplier as Data Processor

(a) The Client appoints the Supplier as its Data Processor of the Client Personal Data.

(b) The Supplier shall Process Client Personal Data only:

(i) on behalf of the Client (and not for itself);

(ii) for the purpose of providing the Services;

(iii) so far as necessary to provide the Services; and

(iv) in accordance with the Client's reasonable and documented instructions from time to time.

(c) The Supplier shall bear its costs of complying with its obligations under this Exhibit.

2.3 Subprocessing

(a) The Client authorises the Supplier to appoint subcontractors as further Data Processors on behalf of the Supplier to Process Client Personal Data (each a "**Subprocessor**"), subject to the requirements set out in the remaining subparagraphs of this paragraph 2.3.

(b) Should the Supplier appoint any Subprocessors, the Supplier shall engage them in writing on terms that:

(i) provide equivalent protections to those set out in this Exhibit; and

(ii) grant the Client the right to perform on the Subprocessor the audits mentioned at paragraph 2.6.

(c) The Supplier shall provide the Client with 30 days' written notice of the proposed addition or replacement of any Subprocessor.

(d) The Client shall have 15 days from the date of receipt of such notice to object to the proposed appointment or replacement of the Subprocessor, on reasonable grounds, by giving written notice to the Supplier.

(e) The Supplier shall, when making a decision whether to appoint or replace any Subprocessor, take into account the Client's representations (if the Client objects to the proposed appointment or replacement of the Subprocessor).

(f) Neither any delay, omission or failure by the Client to object to any proposed Subprocessor, nor any approval by the Client of any Subprocessor (if given), shall relieve the Supplier from any liability or obligation under this Agreement.

(g) The Supplier shall be responsible for the acts, omissions and defaults of any Subprocessor as if they were the Supplier's acts, omissions or defaults.

(h) The Supplier shall:

(i) maintain a list of all Subprocessors that it has engaged to Process Client Personal Data, and of the location of such Subprocessors (including all proposed locations of Processing);

(ii) make such list available to the Client upon request (for example, by making it available on the Supplier's corporate website); and

(iii) at all times keep such list up to date.

2.4 Data Transfers

(a) The Supplier may not Process, nor permit any Subprocessor to Process, Client Personal Data outside the Client's jurisdiction unless:

(i) the Client gives its prior written consent to that Processing (which in the case of Subprocessors the Client shall address by means of the procedure under paragraph 2.3(d) above); and

(ii) the Processing is covered by appropriate safeguards in accordance with applicable law.

(b) The Supplier shall not perform any further transfers of the Client Personal Data outside the Client's jurisdiction beyond the transfer permitted in accordance with paragraph 2.4(a) without complying with the requirements of that paragraph again in respect of such further transfers, and so on.

(c) The Supplier may, where required by applicable law, Process Client Personal Data outside the scope of paragraph 2.4(a) above or otherwise Process Client Personal Data without, or contrary to, the Client's documented instructions. The Supplier shall in such cases provide the Client with advance written notice of the proposed Processing and of the said requirement, except where it is prohibited from doing so by reason of important grounds of public interest.

2.5 Assistance to the Client

(a) Where the Client decides to carry out an assessment of the impact of the Processing or proposed Processing on the protection of Client Personal Data, the Supplier shall upon reasonable request provide assistance to the Client. In particular, at the Client's request the Supplier shall supply the following information:

(i) a systematic description of the way that Client Personal Data is Processed or planned to be Processed;

(ii) a description of the measures it has implemented or plans to implement to protect Client Personal Data and to assist the Client in responding to requests by a Data Subject exercising any of his rights; and

(iii) an assessment (in the form of a Data Protection Impact Assessment), of the specific risks of which the Supplier is aware, to the rights and freedoms of Data Subjects arising out of or in connection with the Processing or planned Processing by the Supplier.

(b) The Supplier shall assist the Client as reasonably requested in cases where the Client decides to carry out a prior consultation with the relevant data protection authority.

2.6 Audit

(a) The Supplier shall upon request provide the Client with all information that the Client reasonably requires in order to demonstrate compliance with applicable Data Protection Law, including SSAE 18 SOC 2 Type II reports (or reports that may replace such standard in the future), covering the Services provided during the period since the previous report.

(b) In addition to the reports detailed in paragraph 2.6(a), the Client may (either itself or (subject to appropriate confidentiality obligations) through its auditors),upon giving reasonable notice and within normal business hours, audit the Supplier's compliance with the terms of this Exhibit.

(c) The Supplier shall assist the Client and its auditors as reasonably required with such audit including by allowing the Client and its auditors access to any relevant premises, personnel and documentation of the Supplier as the Client may reasonably request for such purpose.

(d) The Client shall use all reasonable endeavours to minimise any disruption to the Supplier's business in carrying out any audit pursuant to paragraph 2.6(b).

2.7 Return of Client Personal Data

The Supplier shall, unless applicable law requires the Supplier to retain Client Personal Data, within 14 days of the expiry (or earlier termination) of this Agreement for any reason (or such earlier date as the Client may reasonably request), at no charge to the Client:

(i) return, in a format and on storage media that the Client may reasonably specify, all Client Personal Data that the Supplier (or its Subprocessors) is storing, whether electronically or otherwise, (or is under its (or its Subprocessors') possession or control);

(ii) following the Client's written confirmation of satisfactory receipt of the returned data referred to in paragraph 2.7(i) above, delete or destroy, in such manner as the Client may reasonably request, the Client Personal Data which was the subject of the Client's confirmation of receipt (including destroying relevant copies and back-ups); and

(iii) certify to the Client in writing that all relevant Client Personal Data and media have been successfully returned and destroyed in accordance with this paragraph 2.7.

2.8 Data Subjects' Rights

The Supplier shall:

(i) assist the Client as reasonably required with any communication, request (e.g. subject access request, or request to correct or delete or transmit Personal Data to another Data Controller), objection or any other communication received from Data Subjects, data protection authorities or any other person concerning Client Personal Data, in each case as necessary to enable the Client to respond to any request by a Data Subject exercising his rights or to a data protection authority;

(ii) notify the Client within 1 Working Day if it receives any communication of the type set out in paragraph 2.8(i); and

(iii) not respond directly to any communication of the type set out in paragraph 2.8(i) without the Client's written permission.

2.9 Assistance with Security Events

The Supplier shall assist the Client with any Data Breach and any suspected or threatened Data Breach (each, a "**Security Event**"), including with any required notification to the relevant data protection authority and (if applicable) to Data Subjects by:

(i) notifying the Client immediately (and in any event within 24 hours) of becoming aware of any Security Event, and providing the Client with all relevant information and documentation in its (or its Subprocessors') knowledge, possession or control to enable the Client to notify, if necessary, the relevant data protection authority and, if necessary, Data Subjects. If the

Supplier is unable to provide such information and documentation in the initial notification, the Supplier shall provide it as soon as reasonably practicable thereafter; and

(ii) by co-operating with the Client and (without prejudice to its other obligations under this Exhibit) taking such steps as the Client may reasonably direct to assist in the investigation, mitigation and remediation of any Security Event.

3. **Rights and obligations of the Supplier and the Client – Supplier as either Data Processor or (to the extent permitted in paragraph 4) Data Controller of Client Personal Data**

3.1 This paragraph 3 applies both to the Supplier's Processing of Client Personal Data as a Data Processor, and (to the extent permitted in paragraph 4) to its Processing of Client Personal Data as a Data Controller.

3.2 The Supplier shall:

(i) comply with all applicable Data Protection Law in Processing Client Personal Data; and

(ii) ensure that any person authorised to Process Client Personal Data is bound by contractual obligations of confidentiality.

3.3 The Supplier shall implement and maintain appropriate technical and organisational measures necessary to protect the Client Personal Data from accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure or access, including the measures set out in the Client's information security schedule available at https://www.pmi.com/legal/legal-documents and (without prejudice to the generality of the foregoing), in addition, where appropriate, the following measures:

(a) the pseudonymisation and encryption of Client Personal Data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services;

(c) the ability to restore the availability of, and access to, Client Personal Data in a timely manner in the event of a physical or technical incident; and

(d) a process for regularly testing, assessing and evaluating the effectiveness of the technical and organisational measures for ensuring the security of the Processing.

3.4 The Supplier shall ensure that, having regard to the nature of the Client Personal Data, the technical and organisational measures implemented under paragraph 3.3 take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing, and the risks that are presented by the Processing, in particular from accidental or unlawful destruction, damage, loss, alteration, unauthorised disclosure of, or access to the Client Personal Data.

4. **Rights and obligations of the Supplier and the Client – Supplier as Data Controller of certain Client Personal Data**

4.1 The Supplier may Process on its own behalf (as a Data Controller) Client Personal Data only to the extent that it comprises (i) contact details of personnel of members

of the Client Group; and (ii) login and password data, audit trail data and any similar data generated by or in connection with the system(s), if any, used by the Supplier to provide the Services, in each case only to the extent necessary to Process such data for the purpose of:

(a) exercising its legal rights;

(b) managing its commercial relationship with members of the Client Group, provided this shall not include profiling, or marketing to, individual employees of any member of, or of a supplier to any member of, the Client Group, or making available the Client Personal Data to any third party for any purpose other than as agreed in writing with the Client or as required by applicable law; or

(c) operating such systems and back office processes as are necessary in order to provide the Services.

4.2 The Supplier shall, where it acts as a Data Controller, notify the Client as soon as is reasonably practicable of a Data Breach after becoming aware of the same, and shall (without prejudice to its other obligations under this Exhibit) consult with the Client about such steps as may reasonably be necessary or appropriate to investigate, mitigate and remediate the Data Breach and otherwise assist the Parties to discharge their respective obligations under applicable Data Protection Law.

5. **Rights and obligations of the Supplier and the Client – Client as Data Controller of certain Personal Data relating to Supplier**

5.1 The Client and its Affiliates will Process on their own behalf (each as a Data Controller) certain Personal Data relating to the Supplier, its affiliates, its and their suppliers, and its and their employees. For details, see the Business Partner and Other Stakeholder Privacy Notice available at https://pmiprivacy.com/en/business-partner (as varied or replaced from time to time).

5.2 The Client shall, where it acts as a Data Controller, notify the Supplier as soon as is reasonably practicable after becoming aware of a breach affecting Personal Data relating to the Supplier as Processed by the Client pursuant to paragraph 5.1 above, and shall (without prejudice to its other obligations under this Exhibit) consult with the Supplier about such steps as may reasonably be necessary or appropriate to investigate, mitigate and remediate the Data Breach and otherwise assist the Parties to discharge their respective obligations under applicable Data Protection Law.

5.3 The Client shall bear its costs of complying with its obligations under this Exhibit.

6. **Liability**

6.1 The provisions of the Agreement relating to limitation of liability, and confidentiality in respect of Personal Data, shall remain unaffected except insofar as set out in the remainder of this paragraph 6.

6.2 The following costs ("**Data Protection Losses**") are recoverable as direct losses in respect of a breach of this Exhibit (including a Security Event) involving the Supplier or its Subprocessors (and are not special, incidental, consequential, indirect or punitive damages):

(a) costs of notifying a data protection authority and any other regulator;

(b) costs of notifying affected individuals;

(c) costs of credit monitoring for up to 12 months for affected individuals;

(d) costs of any forensic investigations;

(e) costs of dealing with any investigation by a regulator (including a data protection authority);

(f) legal costs (including those incurred in connection with the above heads of loss);

(g) fines imposed by regulators (including data protection authorities);

(h) costs of reinstating damaged or lost data; and

(i) additional management costs incurred in dealing with the breach.

6.3 Each Party's liability for Data Protection Losses is limited to USD 20 million. The limitations of liability set out in this paragraph 6 shall not apply in case of wilful misconduct or gross negligence, or to the extent mandatory law provides otherwise.