MMC VENDOR DATA PROCESSING AGREEMENT

This Data Processing Agreement ("**DPA**") is made as of the date Supplier first Processes Customer Data on behalf of Customer pursuant to the Principal Agreement ("**Effective Date**") between:

Marsh & McLennan Companies, Inc. and/or its relevant Affiliate ordering Services from the Supplier pursuant to the Principal Agreement ("**Customer**"); and

The provider of the Services identified in the Principal Agreement ("**Supplier**").

In consideration of the mutual obligations set out herein, the Supplier and Customer agree that this DPA and its terms and conditions are attached to and form part of the Marsh & McLennan Companies, Inc.'s Standard Terms and Conditions as attached to the Purchase Order issued by Customer to Supplier, and any statement of work or other ordering document entered pursuant thereto ("**Principal Agreement**"). Capitalised terms used but not defined herein shall have the meaning set out in the Agreement. This DPA consists of (a) the main body of the DPA; (b) the Data Processing Details Addendum at Attachment 1; (c) the Security Terms at Attachment 2; and (d) the Standard Contractual Clauses at Attachment 3 (including Appendices 1 and 2).

1 Definitions

The following terms have the following meanings when used in this DPA:

Affiliate means, with respect to a party, an entity that (directly or indirectly) controls, is controlled by or is under common control with, such party, where control refers to the power to direct or cause the direction of the management and policies of another entity, whether through ownership of voting securities, by contract or otherwise.

Agreement means the Principal Agreement and this DPA.

Cardholder Data, a subset of Personal Data, means credit or debit card account number that identifies the issuer and the particular cardholder account plus any of the following: cardholder name, expiration date and/or service code and sensitive authentication data including security-related information used to authenticate cardholders and/or authorize payment card transactions. The definition of Cardholder Data shall be consistent with the definition of Cardholder Data defined by the current Payment Card Industry Data Security Standards (PCI DSS).

Controller means the entity which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; applicable Data Privacy Laws may use different terms to refer to this entity, including "Business" or "Responsible Party".

Customer has the meaning given it above.

Customer Data means any data, whether in physical or electronic form, including but not limited to documents, databases, records, Personal Data, NPI, intellectual property and confidential information (as defined elsewhere in the Agreement), created by or made available to Supplier in the course of providing Services to Customer and/or any of its Affiliates.

Data Exporter has the meaning given in clause 9.2(b).

Data Importer has the meaning given in clause 9.2(b).

Data Privacy Laws means all laws and regulations applicable to the Processing of Personal Data under the Agreement, including but not limited to U.S. state and federal privacy laws, the GDPR, the

UK Data Privacy Laws, the Brazilian General Personal Data Protection Law, the South Africa Protection of Personal Information Act, the Swiss FADP, the Canadian Protection and Electronic Documents Act (PIPEDA) and provincial privacy laws, all other laws and regulations of in-scope jurisdictions relating to data privacy, as well as any guidance or opinions issued by any Regulator in such jurisdictions.

Data Subject means the individual to whom Personal Data relates.

Data Subject Request means a Data Subject's request by or on behalf of a Data Subject to exercise that person's rights under Data Privacy Laws in respect of that person's Personal Data, including, without limitation, the right to access, correct, amend, transfer, obtain a copy of, object to the processing of, block or delete such Personal Data.

EEA means European Economic Area.

FADP means the Swiss Federal Act on Data Protection, as may be amended from time to time.

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation).

Nonpublic Information (NPI) means electronic Customer Data that is not Publicly Available Information as that term is defined under applicable Data Privacy Laws or regulations.

Personal Data, a subset of Customer Data, means any information made available to Supplier in connection with the Services (i) that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household, or (ii) relating to an identified or identifiable natural person made available to Supplier in connection with the Services; an identifiable natural person, is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to the physical, physiological, mental, economic, cultural or social identity of that natural person.

Personnel means employees, contractors, officers, and directors.

Principal Agreement has the meaning given it above.

Processing or Process means any operation or set of operations which is performed by or on behalf of Supplier as part of the Services upon Personal Data or other Customer Data, whether or not by automatic means, such as collection, recording, organisation, retention, storage, adaptation or alteration, retrieval, consultation, use, disclosure, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Processor means the entity which Processes Personal Data on behalf of the Controller; applicable Data Privacy Laws may use different terms to refer to this entity including but not limited to "Service Provider" or "Operator".

Regulator means the European data protection authority or other regulatory, governmental or supervisory authority with authority over all or any part of (a) the provision or receipt of the Services, (b) the Processing of Personal Data in connection with the Services or (c) Supplier's business or Personnel relating to the Services.

Security Incident means any Personal Data Breach (as defined in Data Privacy Laws) or other incident that has resulted, or is reasonably likely to result, in any accidental, unauthorised or unlawful access to or destruction, loss, theft, alteration, disclosure, acquisition, or encryption of (a) Customer Data or (b) other information under Supplier's control where such incident has the potential to harm Customer's business, clients, employees, systems or reputation.

Services means the services or products to be provided by Supplier to Customer and, as applicable, its Affiliates under the Agreement.

Standard Contractual Clauses means the agreement executed by and between the Data Exporter and Data Importer pursuant to clause 9.2, in the form in the C(2021) 3972 final Annex to the Commission Implementing Decision on 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, of which Module Two (Transfer Controller to Processor) is attached hereto as Attachment 3.

Subcontractor means a third party engaged by or on behalf of Supplier that will Process Customer Data as part of the performance of the Services (including Third Country Recipients).

Supplier has the meaning given it above.

UK Data Privacy 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: (i) the Data Protection Act 2018; and (ii) the UK GDPR.

UK GDPR means The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018, as modified by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019.

2 Relationship with the Agreement

2.1 Supplier's obligations under this DPA are in addition to and not in lieu of its obligations under other provisions of the Agreement. In the event of a conflict between the terms of the Agreement and the terms of this DPA, the terms that afford Customer the greater protection shall apply.

2.2 In the event of a conflict between this DPA and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

3 Processing of Personal Data

3.1 Roles of the Parties

As between Customer and its Affiliates on the one hand and Supplier on the other hand:

(a) Customer or any of its Affiliates may be Controller or a Processor acting on its client's behalf or on behalf of its Personnel, depending on Customer's relationship with the client or Personnel and the relevant Data Subjects;

(b) Where Customer or any of its Affiliates is a Controller, Supplier shall be a Processor; and

(c) Where Customer or any of its Affiliates is a Processor, Supplier shall be sub-processor.

3.2 Customer Affiliates

Supplier shall also provide the Services to, and Process Personal Data provided by or on behalf of Affiliates of Customer, as applicable under the Agreement. In such circumstances, each Affiliate shall be the Controller of the Personal Data that it provides to Supplier and such Affiliate shall have the same rights that Customer has under this DPA when such Affiliate is a Controller in respect of the Personal Data.

3.3 **Supplier's Processing of Customer Data**

(a) Supplier shall Process Customer Data only for the specific and limited purpose of performing the Services and in accordance with Customer's written instructions, shall treat Personal Data as confidential information subject to the confidentiality provisions of the Agreement and will not otherwise use, retain, disclose, transfer or make available in exchange for monetary or other valuable consideration Personal Data to any third parties outside of the direct business relationship with Customer except as necessary to perform the Services. Supplier certifies that it understands the requirements in this paragraph and will comply with them.

(b) Supplier will not combine the Personal Data it Processes on behalf of Customer with any information it collects from another client or individual, unless permitted by the Agreement, a Statement of Work, or Data Privacy Laws.

(c) Customer instructs Supplier to Process Customer Data in accordance with the Agreement and to comply with Customer's other reasonable written (e.g., via email) instructions where such instructions are consistent with the Agreement.

(d) Supplier shall inform Customer immediately if, in Supplier's reasonable opinion, Supplier believes that any instruction given by Customer infringes Data Privacy Laws.

(e) Supplier shall comply with the Data Privacy Laws as they apply to its performance under the Agreement, including by providing the same level of protection for Personal Data as required by the Data Privacy Laws, and Supplier shall not perform the Services in a manner that causes Customer to violate Data Privacy Laws.

(f) The Supplier shall notify Customer if Supplier can no longer meet its obligations under this Agreement or the Data Privacy Laws, and grant Customer the right to take reasonable and appropriate steps to stop and remediate unauthorized use of Customer Data.

(g) If Supplier collects Personal Data directly from the individuals to whom such Personal Data relates on behalf of Customer, Customer reserves the right to require that Supplier post Customer's privacy notice, Supplier's privacy notice, or include additional or modified terms within Supplier's privacy notice.

3.4 **Purpose; Categories of Personal Data and Data Subjects**

The purpose of Processing of Personal Data by Supplier is the performance of the Services pursuant to the Agreement. The types of Personal Data and categories of Data Subjects Processed under this DPA are further specified in Attachment 1 (*Data Processing Details Addendum*).

3.5 **Limitation on Disclosure**

Other than as expressly permitted by the Agreement, instructed in writing (including by email) by the Customer or required by law, Supplier shall not disclose Customer Data to any third parties without Customer's prior written consent.

4 Data Subject Rights; Other Complaints and Requests

4.1 **Data Subject Requests**

(a) Supplier shall notify Customer of a Data Subject Request promptly but in any event not later than 3 days following Supplier's receipt of the Data Subject Request. Supplier shall not respond to any such Data Subject Request without Customer's prior written instructions and, to the extent permitted by such Data Privacy Laws, shall inform Customer of any legal

requirement before Supplier responds to the Data Subject Request; or direct the requesting individual to submit the Data Subject Request directly to Customer as set out in the privacy notice on Customer's website from time to time.

(b) Supplier shall provide such assistance, and notify Subcontractors of their obligation to assist Customer, and take such action as Customer may reasonably request (including assistance by appropriate technical and organisational measures) to allow Customer to fulfil its obligations to clients or under Data Privacy Laws in respect of Data Subject Requests, including, without limitation, meeting any deadlines imposed by such obligations.

4.2 Other Complaints and Requests

(a) Supplier shall notify Customer promptly but in any event not later than 3 days following receipt of any complaint or request (other than Data Subject Requests or enquiries of Regulators described in Section 0) relating to (a) Customer's obligations under Data Privacy Laws or (b) Personal Data.

(b) Supplier shall promptly provide such co-operation and assistance as Customer may request in relation to such complaint or request.

5 Supplier Personnel

Supplier shall ensure that its Personnel engaged in Processing of Customer Data are informed of the confidential nature of the Customer Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements in respect of the Customer Data that survive termination of the Personnel engagement. Supplier shall be responsible and liable for the acts, omissions or defaults of its Personnel in the performance of obligations under this DPA or otherwise as if they were Supplier's own acts, omissions or defaults.

6 Subcontractors

6.1 Appointment of Subcontractors

Supplier may engage Subcontractors solely in connection with the provision of the Services, subject to clause 3.5, clause 6.22 and the other provisions of the Agreement.

6.2 Subcontractor Agreements

Supplier shall ensure that the subcontract entered into with any Subcontractor imposes on the Subcontractor the same obligations as those to which Supplier is subject under this DPA.

6.3 List of Current Subcontractors and Notification of New Subcontractors

(a) Upon request, Supplier shall provide Customer with a current list of the names and contact information of any Subcontractors (the "**Subcontractor List**"). Supplier shall provide sixty (60) days' prior notice by email to Customer of any addition of a new Subcontractor to the Subcontractor List.

(b) If Customer objects to Supplier's proposed use of a new Subcontractor, Supplier will use reasonable efforts to refrain from permitting such proposed Subcontractor to Process Customer Data without adversely impacting the Services or Customer. If Supplier determines that it cannot avoid such an adverse impact despite such reasonable efforts, Supplier shall notify Customer of such determination. Upon receipt of such notice, Customer may terminate all or any part of the Agreement without penalty or liability (other than for fees due and owing to Supplier for Services performed prior to such termination) effective immediately upon the

termination date specified in Customer's written notice of such termination to Supplier. Supplier shall refund Customer any prepaid fees for the period following the effective date of termination.

6.4 **Responsibility for Subcontractors**

Supplier shall be responsible and liable for the acts, omissions or defaults of its Subcontractors in the performance of obligations under this DPA or otherwise as if they were Supplier's own acts, omissions or defaults.

7 Security

7.1 Supplier shall take appropriate technical and organisational measures to ensure the confidentiality, integrity, availability and resilience of Supplier systems used for Processing Customer Data and protect against the unlawful destruction, loss, alteration, unauthorised disclosure of or access to Personal Data transmitted, stored or otherwise Processed. Without limiting the generality of the foregoing, Supplier shall comply with the requirements set out in Attachment 2 (*Security Terms*), including its obligation to notify Customer of Security Incidents.

7.2 **Cardholder Data**

(a) To the extent Supplier processes Cardholder Data under the Agreement or an applicable Statement of Work, Supplier represents and warrants that it is and will remain in compliance with all applicable PCI DSS requirements, and will provide Customer with annual evidence of the same in the form of its Payment Card Industry Attestation of Compliance.

(b) If at any time Supplier becomes aware that it is unable to comply with or mitigate the risk associated the applicable PCI DSS requirements, Supplier with notify Customer within 10 days. Nothing in this paragraph alters Suppliers' Security Incident reporting obligations.

(c) To the extent PCI DSS requirements conflict with any requirements in Attachment 2 (*Security Terms*), Supplier shall protect Cardholder Data in accordance with PCI DSS requirements.

8 Audits

Supplier shall comply with the audit requirements set out in Attachment 2 (*Security Terms*).

9 Transfers Outside of the Country of Origin

Restrictions on Transfer

(a) Supplier shall not permit:

(i) Personal Data originating in the UK, Switzerland or the EEA to be Processed outside the UK, Switzerland or the EEA as applicable; or

(ii) Personal Data originating in a country outside the UK, Switzerland or the EEA to be Processed in a different country, without Customer's prior written consent, other than to the extent expressly permitted by the Agreement.

(b) Supplier shall ensure that any Personal Data that originated from the UK, Switzerland or the EEA and is Processed outside the UK, Switzerland or the EEA pursuant to Customer's prior written consent complies with clause 9.2.

(c) Supplier shall ensure that any transfer of Personal Data originating in a non-UK, Switzerland or EEA country and is Processed in another country pursuant to Customer's prior written consent complies with clause 9.3.

9.2 **Application of Standard Contractual Clauses**

(a) Module Two (Transfer Controller to Processor) of the Standard Contractual Clauses and the additional terms in this clause 9 will apply to Processing of Personal Data that is transferred from within the EEA, the United Kingdom (subject to Attachment 4 – UK Addendum to the EU Standard Contractual Clauses), Switzerland (Subject to Attachment 5 – Switzerland Addendum to the EU Standard Contractual Clauses), or any other jurisdiction which accepts the Standard Contractual Clauses (subject to Section 9.2(e) below), either directly or via onward transfer, to any recipient (i) not located in a country recognised by the European Commission or the UK Government as applicable as providing an adequate level of protection for Personal Data or (ii) not covered by a framework recognised by the relevant authorities or courts as providing an adequate level of protection for Personal Data, including but not limited to Binding Corporate Rules or the Trans-Atlantic Data Privacy Framework (each such recipient, a "**Third Country Recipient**").

(b) The Standard Contractual Clauses shall be deemed executed by virtue of deemed acceptance by conduct of the Principal Agreement by Supplier providing the Services and Customer paying for such Services in accordance with the purchase order to which the Principal Agreement is attached, by:

(i) Customer and/or any Affiliate to whom Supplier provides the Services that transfers Personal Data to a Third Country Recipient (the "**Data Exporter**"); and

(ii) Supplier or other relevant Third Country Recipient (the "**Data Importer**").

.

(c) The Standard Contractual Clauses shall constitute a separate agreement between each Data Exporter and Data Importer. If so required by Data Privacy Laws, the parties shall execute or re-execute the Standard Contractual Clauses as separate documents setting out the proposed transfers of Personal Data in such manner as may be required by Data Privacy Laws.

(d) The parties agree to amend the Standard Contractual Clauses if required in accordance with a relevant European Commission or UK/Swiss government decision or Data Privacy Laws. Nothing in this DPA or the Agreement shall contradict, directly or indirectly, the Standard Contractual Clauses, or prejudice the fundamental rights or freedoms of Data Subjects. In the event of such a contradiction, the Standard Contractual Clauses shall prevail.

(e) Where the Standard Contractual Clauses apply to a transfer of Personal Data from any other jurisdiction which accepts the Standard Contractual Clauses as appropriate safeguards under Data Privacy Laws, Annex 6 (Transfer Requirements for Other Jurisdictions) shall apply, and any amendments required by such jurisdiction's Regulator shall be deemed to be made to the Standard Contractual Clauses as are necessary to comply with Data Privacy Laws.

(f) The following sections of this DPA shall apply to the Standard Contractual Clauses, provided that these shall not operate to contradict the Standard Contractual Clauses:

(i) For the purposes of the Standard Contractual Clauses, the instructions to Data Importer shall be any instructions issued in accordance with Section 3.3(a) of this DPA.

(ii) Section 4.1 of this DPA shall apply to any enquiries or requests that the Supplier receives from a Data Subject that the Supplier is obliged to deal with in accordance with Clause 10 of the Standard Contractual Clauses.

(iii) Section 4.2 of this DPA shall apply to any complaints that the Supplier receives from a Data Subject that the Supplier is obliged to deal with in accordance with Clause 11 of the Standard Contractual Clauses.

(iv) Section 6 of this DPA shall apply in respect of any sub-processing by the Data Importer.

9.3 **Controls on transfers not covered by the Standard Contractual Clauses**

Where the Supplier transfers Personal Data originating in a non-EEA or non-UK country to another country, it shall:

(a) put in place reasonable, appropriate and legally compliant safeguards for protection of such Personal Data in accordance with good industry practice;

(b) to the extent required by applicable Data Privacy Law, enter into (or procure the entry into) such agreement with the Customer or, if applicable, the Customer Affiliate, as requested by the Customer; and

(c) comply with, and assist the Customer or, if applicable, the Customer Affiliate to comply with, any other obligations under applicable Data Privacy Law relating to the transfer.

The Supplier shall also ensure that any onward transfer of Personal Data originally transferred pursuant to this clause 9.3 shall be made in compliance with the requirements of the applicable Data Privacy Law and, if applicable, the data transfer mechanism relied upon pursuant to this clause 9.3.

9.4 **Transfer Risk Assessment and Supplementary Measures**

(a) The Supplier shall support Customer to ensure compliance with Data Privacy Laws and other applicable law for the transfer of Personal Data of Data Subjects located in the UK, Switzerland or the EEA to third countries including by undertaking and documenting a transfer risk assessment in accordance with Data Privacy Laws and the Standard Contractual Clauses before first transferring Personal Data and then no less than annually and the Supplier shall deliver such completed transfer risk assessment promptly to Customer upon request.

(b) The Supplier shall ensure that the appropriate technical and organizational measures it implements and maintains as required by the Standard Contractual Clauses, address the risks associated with the transfer of Personal Data to a third country and the Supplier shall implement any further additional safeguards required by its transfer risk assessment and/or as agreed with Customer.

(c) The Supplier warrants on an ongoing basis that it is able, through the implementation of appropriate technical and organizational measures, to satisfy its obligations under the Standard Contractual Clauses and this DPA.

(d) The Supplier certifies that: (i) it has not and will not create back doors (non-transparent access capabilities) or similar programming that could be used to access its systems and/or the Personal Data; (ii) it has not and will not change its business processes in a way which facilitates unauthorized access to its systems and/or the Personal Data; and (iii) applicable law does not require the Supplier to create or maintain back doors or to facilitate unauthorized access to its systems and/or the Personal Data or for the Supplier to be in possession of or to hand over to any third party keys to decrypt the Personal Data.

(e) In the event that the Supplier or any of its Subcontractors receives an order from any third party for compelled disclosure of any Personal Data Processed under this DPA, Supplier and its relevant Subcontractor shall:

(i) redirect the third party to request the data directly from Customer;

(ii) promptly notify Customer, unless prohibited under applicable law, in which case Supplier shall use all lawful efforts to waive the prohibition and shall communicate as much information to Customer as soon as possible; and

(iii) use all lawful efforts to challenge the order for disclosure on the basis of any legal deficiencies under the applicable laws or any relevant conflicts with Data Privacy Laws.

9.5 **Changes in Data Privacy Laws**

Should a change in Data Privacy Laws occur, or a decision of a competent authority in connection with Data Privacy Laws be made, which might affect the validity of an international transfer or adequacy of an international transfer method (including, but not limited to, the Standard Contractual Clauses), then the Supplier agrees to promptly co-operate (and ensure that any affected Subcontractors promptly co-operate) with Customer to ensure that any variations or other agreements necessary to restore such validity or adequacy are promptly agreed to allow such international transfers to be made (or continue to be made) without breach of that change or decision regarding that Data Privacy Law.

10 Co-operation with Regulators and Conduct of Claims

10.1 Supplier shall promptly notify Customer of all enquiries from a Regulator that Supplier receives which relate to the Processing of Customer Data, the provision or receipt of the Services or either party's obligations under this DPA, unless prohibited from doing so at law or by the Regulator.

10.2 Unless a Customer notifies Supplier that Supplier will be responsible for handling a particular communication or correspondence with a Regulator or a Regulator requests in writing to engage directly with Supplier, Customer will handle all communications and correspondence relating to Customer Data and the provision or receipt of the Services.

10.3 Customer shall have the right, at its sole discretion, to assume control of the defence and settlement of any third-party claim that relates to the Processing of Personal Data, including claims against Supplier or its Subcontractors, provided that Customer shall not enter into any settlement of such claim or compromise any such claim without Supplier's prior written consent if such compromise or settlement would assert any liability against Supplier, increase the liability (including under an indemnity) of Supplier, or impose any obligations or restrictions on Supplier, such as imposing an injunction or other equitable relief upon Supplier. Where required, such consent shall not be unreasonably withheld or delayed. Customer's exercise of such right under this clause 10.3 shall (a) not be construed to require Customer to bear the costs of such defence and settlement and (b) be without prejudice to its contractual, legal, equitable or other rights to seek recovery of such costs.

10.4 Where Supplier interacts directly with a Regulator in accordance with clause 10.2, Supplier shall do so in an open and co-operative way at its own expense and in consultation with Customer. With respect to such interaction with a Regulator, Supplier shall (and shall cause its personnel and Subcontractors to):

(a) make itself readily available for meetings with the Regulator as reasonably requested;

(b) subject to clause **Error! Reference source not found.** below, answer the Regulator's questions truthfully, fully and promptly; and provide the Regulator with such information and co-operation as the Regulator may require; and

(c) where permitted by law, notify Customer of any Regulator's request for information relating to Customer or the Personal Data and before disclosing such requested information, co-operate with Customer's efforts to prevent the disclosure of, or obtain protective treatment for, such information, and comply with Customer's reasonable instructions regarding the response to such request. Any confidential information disclosed by the Supplier in accordance with clause 10.4 shall be disclosed subject to the Agreement's confidentiality provisions.

10.5 Supplier shall provide Customer with such assistance and information as Customer may reasonably request in order for Customer to comply with any obligation to carry out a data protection impact assessment or consult with a Regulator pursuant to Articles 35 and 36 of GDPR, respectively.

11 Indemnity

Supplier shall, at all times during and after the termination or expiration of the Agreement, indemnify, defend, and hold harmless Customer and its Affiliates and their respective Personnel and agents against any and all losses, damages, costs or expenses and other liabilities (including legal fees) arising out of or in connection with (a) any breach of this DPA, or the negligence or wilful misconduct in the performance of this DPA, by Supplier, its Personnel, Subcontractors, or agents or (b) any Security Incident.

12 Termination and General

12.1 This DPA and the Standard Contractual Clauses will terminate when Supplier ceases to Process Customer Data, unless otherwise agreed in writing between the parties. On termination of the DPA for whatever reason, or upon written request from Customer at any time, Supplier shall cease to use or Process any Customer Data and comply with its obligations under paragraph 2.6 of Attachment 2 (*Security Terms*).

12.2 **Liability**

The parties agree that no limitations of or exclusions from liability set out in the Agreement will apply to (A) any party's liability to Data Subjects under the third-party beneficiary provisions of the Standard Contractual Clauses to the extent limitation of such rights is prohibited by Data Privacy Laws; or (B) the obligations set forth under Section 11, Indemnity, above.

12.3 **Governing Law**

To the extent required by applicable Data Privacy Laws (e.g., in relation to the governing law of the Standard Contractual Clauses), this DPA shall be governed by the law of the applicable jurisdiction. In all other cases, this DPA shall be governed by the laws of the jurisdiction specified in the Agreement.

13 Legal Effect

This DPA shall take effect between, and become legally binding on, the parties as of the Effective Date by virtue of Supplier providing the Services in accordance with the Principal Agreement which incorporates this DPA by reference.

ATTACHMENT 1

Data Processing Details Addendum

This Attachment forms part of the DPA and must be completed by the parties

Data subjects
The Personal Data Processed concern the following categories of data subjects (please specify):
Customer and its Affiliates' personnel together with any other categories of data subjects contemplated by the Principal Agreement.

Categories of data
The Personal Data Processed concern the following categories of data (please specify):
Business contact information together with other categories of data contemplated by the Principal Agreement.

Special categories of data (if appropriate)
The Personal Data Processed concern the following special categories of data[1] (please specify):
None unless contemplated by the Principal Agreement.

Processing operations
The Personal Data Processed will be subject to the following basic processing activities (please specify):
As necessary to provide the Services as set out in the Principal Agreement **.**

[1] Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, processing of genetic data, biometric data for the purposes of uniquely identifying a natural person, data concerning health or data concerning and natural person's sexual orientation, data regarding criminal convictions.

ATTACHMENT 2

Security Terms

The terms and conditions in this attachment (the "**Security Terms**") shall apply when, during the course of providing Services to Customer, Supplier (a) Processes Customer Data or (b) requires access to Customer's computer network or telecommunications systems ("**Customer Network**"). In the event that the provisions of these Security Terms conflict with security, data protection, or network access requirements elsewhere in this DPA or in a Statement of Work, the terms that afford Customer the greater protection shall apply. Nothing in these Security Terms is intended to limit or relieve Supplier of its most basic obligation to implement and maintain an effective information security program.

1 Definitions

1.1 **Industry Standard Safeguards** means those safeguards widely accepted by information security professionals as necessary to reasonably protect data during Processing consistent with the sensitivity of and widely recognised threats to such data. Examples of Industry Standard Safeguards include those practices described in ISO/IEC 27002:2013, NIST CSF, Microsoft Security Hardening Guides, OWASP Guide to Building Secure Web Applications, and the various Center for Internet Security (CIS) Standards.

1.2 **Multi-Factor Authentication (MFA)** means authentication through verification of at least two of the following types of authentication factors: (i) knowledge factors, such as a password; or (ii) possession factors, such as a token or text message on a mobile phone; or (iii) Inherence factors, such as a biometric characteristic.

1.3 **Risk-Based Authentication** means any risk-based system of authentication that detects anomalies or changes in the normal use patterns of a person and requires additional verification of the person's identity when such deviations or changes are detected, such as through the use of challenge questions.

1.4 Other capitalised terms used and not defined in these Security Terms have the respective meanings given in the DPA or elsewhere in the Agreement.

2 General Information Security Standards

2.1 Supplier represents and warrants that

(a) it has in place and will maintain a comprehensive, written information security program pursuant to which it has implemented administrative, technical and physical safeguards designed to: (1) ensure the confidentiality, integrity, availability and security of Customer Data; (2) protect against any foreseeable threats or hazards thereto; (3) protect against unauthorised, accidental or unlawful access to or use of Customer Data and Supplier systems; (4) protect against unauthorised, accidental or unlawful destruction, loss, alteration, encryption or misuse of Customer Data and (5) ensure that Supplier's Personnel and Subcontractors are appropriately trained to maintain the confidentiality, integrity, availability and security of Customer Data, consistent with the terms of the DPA, these Security Terms, any Statement of Work, other provisions of this Agreement and all applicable laws and regulations;

(b) Such safeguards will include, without limitation, the application of Industry Standard Safeguards to protect Supplier's systems used to Process Customer Data, and to limit access to Customer Data to only those employees, agents or Subcontractors of Supplier who need the information to carry out the purposes for which Customer Data was disclosed to Supplier;

(c) Such safeguards are no less rigorous than those used by Supplier for its own information of a similar nature; and

(d) Supplier is in and will remain in compliance with its information security program in all material respects.

2.2 Supplier represents and warrants that prior to permitting any Subcontractor to access Customer Data, Supplier shall conduct a reasonable, documented investigation of such Subcontractor to verify that it is capable of maintaining the privacy, confidentiality and security of Customer Data in compliance with this DPA, a Statement of Work (if applicable), and these Security Terms, and will impose on the Subcontractor obligations concerning Customer Data substantially similar to, but no less restrictive than, the obligations applicable to Supplier under this DPA. Upon Customer's request, Supplier shall promptly provide to Customer evidence of the foregoing.

2.3 Supplier will designate an individual who will serve as Customer's ongoing point of contact for purposes of addressing issues with respect to the use and security of Customer Data during the term and following the termination or expiration of this DPA and/or the Statement of Work. Such individual will be accessible to Customer and will cooperate with Customer to address such issues.

2.4 Without limiting the foregoing, Supplier represents and warrants that it has implemented and will maintain the following minimum controls with respect to Customer Data in accordance with Industry Standard Safeguards:

(a) Organisational and technical measures designed to ensure that Customer Data is not Processed by Supplier or its Subcontractors for any purposes other than for the performance of the Services under the Agreement.

(b) Periodically updated inventories of (a) Personal Data that Supplier Processes and (b) Supplier systems that process Personal Data.

(c) Logical access controls to manage access to Customer Data and system functionality on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, unique IDs and passwords, Multi-factor Authentication or equally protective Risk-Based Authentication for system administrators and any remote access to its network and internal systems, and promptly revoking or changing access in response to terminations or changes in job functions.

(d) Password controls to manage and control password complexity, expiration and usage for all user accounts associated with access to Customer Data, whether directly or indirectly, including blocking user access after multiple unsuccessful password attempts and terminating sessions after a predetermined period of inactivity. Any password controlling access to Customer Data must be at least 8 characters in length, including a reasonable level of complexity, and a maximum expiration threshold of ninety (90) days.

(e) Customer Data is logically or physically segregated from any other data of Supplier or its customers.

(f) Physical controls to protect information assets from environmental hazards and unauthorised access, and to manage and monitor movement of persons into and out of Supplier's facilities where Customer Data is stored, processed, or transmitted.

(g) Operational procedures and controls to ensure technology and information systems are configured and maintained according to prescribed internal standards.

(h) Application security and software development controls designed to prevent the introduction of security vulnerabilities in any software developed by Supplier.

(i) Network security controls, including the use of firewalls, layered DMZs, and updated intrusion detection/prevention systems to help protect systems from intrusion and limit the scope or success of any attack or attempt at unauthorised access to Customer Data.

(j) Vulnerability management and regular application, operating system and other infrastructure scanning and patching procedures and technologies to identify, assess, mitigate and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

(k) Encryption of Customer Data in accordance with the requirements as set forth in Section 3 Data Protection of these Security Terms and using appropriate algorithms and key lengths to reasonably protect Customer Data against unauthorised access, disclosure, or theft.

(l) Business resiliency/continuity and disaster recovery procedures to ensure Supplier's ability to maintain service and recover from foreseeable emergency situations or disasters in a timely manner.

(m) Change management procedures to ensure all modifications to Supplier's technology and information assets are properly tested, approved, recorded, and monitored.

(n) Incident management procedures to allow for the proper investigation, response, mitigation and notification of events related to the confidentiality, integrity, and availability of Supplier's technology and information assets.

(o) Organisational management to ensure the proper development and maintenance of information security and technology policies, procedures and standards.

(p) Background checks (including criminal background checks) of any Personnel who may gain access to Customer Data that are repeated at adequate intervals, and administrative controls to ensure no one convicted of a crime of dishonesty, breach of trust, or money laundering is permitted to access Customer Data.

(q) Ensure no individual who has been convicted of a crime of dishonesty, breach of trust, or money laundering has access to Personal Data.

(r) Use of secure destruction procedures following NIST Media Sanitization standards (NIST 800-88 current revision) to sanitise any unencrypted hard disk, portable storage device or backup media containing Customer Data prior to sending it offsite for maintenance or disposal purposes.

2.5 Supplier shall promptly notify Customer in advance of any changes in the controls or other safeguards that would result in a material weakness in, or have an adverse impact on, the security of Customer Data.

2.6 Work from Home Activity: In the event any Supplier offshore staff working remotely on full-time basis (e.g., working from home during pandemics or as part of Supplier's standard organizational structure), the following additional requirements apply and which form a part of this Agreement which Supplier has entered into with Customer. In consideration of the obligations set out herein, and in the event any Supplier offshore staff are working remotely on full-time or short-term basis (e.g., working from home as part of Supplier's standard organizational structure or during pandemics, events of civil unrest or other events that may prevent Supplier personnel from physically working on-site or from within Supplier's corporate and business service locations) ("WFH Activity"), the terms in this Section

2.6 shall apply. Supplier's obligations in this Section 2.6 are in addition to its obligations under applicable law and its other obligations under the DPA. In the event of a conflict between the terms of the DPA and these WFH Activity terms, the terms which are more protective of Customer Data and Customer's network and systems shall control. Defined terms used herein have the meaning given to them in the DPA as appropriate. Supplier shall ensure that at all times during any WFH Activity:

(a) N Supplier personnel are required to have acknowledged and signed an Acceptable Use of Information Assets Policy which is sufficient to protect Customer's information assets, including Customer Data, before commencing any WFH Activity and Supplier shall provide evidence of such Policy and signatures promptly upon request by Customer;

(b) browsing controls on endpoints used to connect to Customer's network or used to process Customer Data must be configured to restrict browsing capabilities only to what is necessary to provide the Services when working remotely and to prevent the upload of data or use of social media sites or webmail;

(c) only Supplier-provided (e.g., "Corporate assets") may be used to connect to Supplier's network and systems used to provide the Services;

(d) multi-factor Authentication (MFA) or one-time passwords must be in place for all remote access to Supplier's network and systems (for avoidance of doubt, MFA shall not include use of solutions that provide the MFA via SMS or email);

(e) computer screens and remote access sessions must be configured for idle timeout (i.e., endpoints must be configured with password protected screen locks that invoke after 15 minutes of inactivity and the VPN access must be reauthenticated at least every 24 hours for active connections);

(f) all endpoints must be configured to prohibit access to and use of removable media and use of screenshot or screen snapshot utilities or features;

(g) local printing functions must be disabled (i.e., Supplier personnel must be prevented from printing to personally-owned or local printers); and

(h) Supplier personnel should have a regular semi-private workspace (i.e., no at-home workspace should be shared with other working family members; no working from public areas such as coffee shops, internet cafes, airports, etc. unless it is necessary to do so on occasion, in which cases privacy screens and/or similar solutions must be implemented where any members of the general public may be present. Regular working in public areas is prohibited).

2.7 On termination of this DPA for any reason or upon request, Supplier will cease Processing Customer Data and require its Subcontractors to do the same, return a copy of the Customer Data to Customer upon request, and then securely delete or destroy, as applicable, all Customer Data in Supplier's possession (except as prohibited by law or other explicit data retention and/or return provisions in this DPA). To the extent any Customer Data is retained by Supplier or where destruction of Customer Data is infeasible, Supplier's confidentiality and security obligations shall continue in accordance with the Agreement for as long as Supplier retains Customer Data.

3 Encryption

3.1 Supplier will encrypt or shall provide features for Customer to encrypt all Customer Data, at no additional cost to Customer, in accordance with the table below using current, industry-standard algorithms and key lengths to protect Customer Data against unauthorised access, disclosure, or theft during any physical or logical transfer or storage, and as further described below:

Process	Minimum Acceptable Encryption Method(s)	Example Solutions(s)
Customer Data transfer across any public network, including the Internet	IPSec, TLS 1.2 or higher between hosts with minimum 128-bit symmetric key; 2048-bit asymmetric key. *Solutions such as Dropbox are not permitted.*	sFTP, OpenSSL, IPSec VPN tunnel
Transfer of Personal Data or NPI in e-mail message body (i.e. non-bulk)	TLS transport layer encryption between e-mail gateways of Supplier and Customer	TLS
Transfer of Personal Data or NPI via e-mail attachment (i.e. bulk transfer greater than 5 identities)	Encrypted attachment or point to point e-mail encryption solution.	S/MIME, PGP, WinZip (AES-256) w/15-character passphrase delivered using alternate communications method
Customer Data storage or transfer using portable devices (e.g. CD/DVD, laptop hard disks, PDA's, memory cards/sticks)	'Whole Disk' encryption or volume encryption using AES-256 with a minimum 15-character passphrase or two-factor authentication token required to decrypt.	McAfee Drive Encryption, PGP Whole Disk, Mobile Armor, Microsoft BitLocker
Personal Data or NPI storage on removable archival media (i.e. backup tapes)	Personal Data written to tape in encrypted form using Industry Standard algorithm, and/or full tape encryption with appropriate key management.	Decru DataFort, NetBackup encryption, CommVault encryption, tape drive hardware encryption, PGP Archive containing Personal Data is written to backup tape.
Personal Data or NPI stored on file servers or in application databases	File, container, or record level encryption using Industry Standard algorithm with appropriate access controls and key management.	Microsoft EFS, SQL column encryption, PGP File or PGPDisk, TrueCrypt, WinZip encrypted archive.

3.2 Without limiting the foregoing, Supplier represents and warrants that in the absence of prior express written permission from Customer it will not store Personal Data or NPI on any portable storage device.

3.3 If at any time Supplier receives Personal Data or NPI from Customer that is not protected in accordance with these Security Terms, Supplier will immediately notify Customer so that prompt remedial action can be taken.

4 Supplier Access to Customer Network and Systems

4.1 If applicable to or required for the Services, Supplier access to Customer's computer network and/or telecommunications systems ("Customer Network") shall be subject to the following terms and conditions:

(a) Supplier's authorisation to use the Customer Network is specifically conditioned upon compliance with any technical requirements in these Security Terms, other provisions of this DPA and as may be provided to Supplier by Customer in writing with respect to the access method. Supplier shall not cause, permit, or authorise any change, modification,

enhancement, or additions to such technical requirements without the prior written consent of Customer. Supplier agrees that Customer reserves the right to monitor Supplier's computer system(s) or other source device(s) while such device(s) are actively connected to or communicating with Customer's Network or equipment, and intercept Supplier's communications traversing the Customer Network or equipment at any time and without prior notice. Supplier agrees that Customer may further impose certain technical requirements or limitations upon Supplier's access and/or Supplier's computer system(s) for purposes of access to the Customer Network in accordance with Customer's third-party connectivity standards such as may be required for establishing business-to-business (B2B) or other direct connections to Supplier's computer(s), including requiring Supplier to provide to Customer the names of Supplier Personnel assigned to perform the Services. Supplier shall notify Customer immediately of any changes in such Supplier Personnel in order to permit Customer to promptly revoke access of Supplier Personnel to Customer's systems and Customer's Network. If Customer grants Supplier access to the Customer Network via Supplier's computer or other Supplier access device, Supplier agrees that prior to beginning such access it will have installed and activated up-to-date security products on such device, including but not limited to a host intrusion prevention software or firewall, full disk encryption in accordance with these Security Terms and comprehensive anti-malware software (including virus and spyware protection). If Supplier becomes aware of any security issue (e.g. malware infection) with its access device while connected to the Customer Network, Supplier will disconnect immediately and notify Customer promptly (but not more than 24 hours upon discovery).

(b) Supplier's access to the Customer Network and associated applications shall be solely for the purpose of providing designated Services to Customer. Supplier shall not use the Customer Network, directly or indirectly, for any of the following purposes:

(i) to transmit to or receive from or communicate with networks, persons or entities other than Customer and its officers and employees, except with prior written consent of Customer (for example, one Supplier location may not use the Customer Network to communicate directly or indirectly with other Supplier locations);

(ii) to establish a peer-to-peer network connection between Supplier's computer and any computer on the Customer Network, the Internet, or Supplier's own network, without Customer's prior written consent;

(iii) to use third-party e-mail or file transfer services (e.g., Hotmail, Yahoo, AOL, Google, Dropbox, etc.);

(iv) to conduct any kind of business or transaction other than with, or for the benefit of, Customer;

(v) to copy or transfer Customer Data outside of Customer's Network other than expressly set forth in the Agreement in performance of the Services;

(vi) to accomplish any illegal or unlawful purpose, or to do any activity which would violate any law, rule, regulation, ordinance, or decree of any governmental authority, or cause Customer to be in violation of any such law, rule, regulation, ordinance, or decree, or which could subject Customer to any sanction, civil or criminal;

(vii) to access any data and/or network to which Supplier does not have prior authorisation from Customer;

(viii) to upload, post, e-mail, otherwise transmit, or post links to any material that contains malicious software, bots, viruses, spam, time bombs, trap doors or any other computer code, files or programs or repetitive requests for information designed to intercept,

transmit, or otherwise gain unauthorised access to information or to interrupt, destroy or limit the functionality of the Customer Network, telecommunications equipment, or data, or any other party's network, or to diminish the quality of, interfere with the performance of, or impair the functionality of the Customer Network or any other party's network;

(ix) to infringe or to misappropriate any patent, trademark, copyright, moral right, trade secret, or other similar right of Customer or any third party;

(x) to access any information that is confidential or proprietary to Customer, its clients, or its third-party licensors or contractors, except on a "need to know" basis in connection with the Services;

(xi) to violate any agreement between Supplier and Customer;

(xii) to knowingly cause Customer to violate any agreement between Customer and any third party; or

(xiii) to use words, phrases or symbols that may be viewed as inappropriate, offensive, defamatory, harassing or otherwise compromising to any person.

5 Risk Assessments and Security Audits

5.1 Supplier will perform regular (i.e. at least quarterly) vulnerability tests and assessments against all systems Processing Customer Data, and shall perform regular (i.e. at least annually) penetration tests against any Internet-facing systems used in connection with the Services. Supplier further agrees to perform regular (i.e. at least annually) risk assessments of the physical and logical security measures and safeguards it maintains applicable to its protection of Customer Data. With respect to systems Processing Customer Data, Supplier will provide Customer, upon request, a summary report of such tests and assessments, including a description of any significant (i.e. moderate or greater) risks identified and an overview of the remediation effort(s) undertaken to address such risks.

5.2 In addition to any other audit obligations that may be contained in this DPA or a Statement of Work, Customer or its designated third party, at its sole expense, may inspect, audit, review, scan, assess, and/or test (i) Supplier's information security and privacy policies, practices, procedures and technical or organizational measures applicable to Supplier's duties under this Exhibit and the systems, applications, and facilities Processing Customer Data, including data centres or premises where the Personal Data is stored, Processed, or accessed from ("**Inspection**"). Supplier shall make relevant Personnel available for interviews and provide all information and assistance reasonably requested by Customer in connection with any such Inspections, including, without limitation, such information as Customer requires to verify compliance with this DPA and Data Privacy Laws. The methods Customer uses to complete such inspections may include Supplier's completion of an online or offline questionnaire form, or providing Customer with alternative industry standard risk assessment reports or completed forms, as may be deemed acceptable by Customer in its sole discretion (e.g. industry standard assessment reports or material means SOC 2 Type II audit reports, and/or other third party certifications such as PCI-DSS Certification, ISO 27001:2013 Certification, and/or the most current version of published SIG or CAIQ Forms). Following the Inspection, Supplier shall take such remedial actions as are reasonably required by Customer, including as may be required by applicable law. Barring exigent circumstances such as Customer's reasonable concern of an actual breach or imminent material breach of security or processing of Personal Data by Supplier in a manner that would violate or cause Customer to violate Data Privacy Laws, such Inspections may occur no more than once in any twelve (12) month period and Supplier will be given not less than thirty (30) days' prior written notice.

6 Security Breaches and Incident Response

6.1 Supplier agrees to notify Customer immediately (but in no case later than 24 hours) after learning of a Security Incident. Notification must include a phone call to Supplier's primary account contact, relaying all details described in Section 6.2 below. In the event Supplier is unable to reach such contact within such 24-hour period, Supplier must send notification of the Security Incident to IncidentReporting@mmc.com.

6.2 Notification shall include at a minimum (a) a description of the Security Incident including impact and likely consequences thereof and, where possible, the categories and approximate number of data subjects and Personal Data records concerned, (b) the expected resolution time (if it has not already been resolved), (c) a description of corrective measures to be taken, evaluation of alternatives, and next steps, including, where appropriate, measures to mitigate its possible adverse effects, (d) whether any regulatory authority, the Data Subjects or the media have been informed or are otherwise already aware of the Security Incident, and their response, and (e) the name and phone number of the Supplier representative that Customer may contact to obtain further information and updates. If not available at the time of initial notification to Customer, Supplier shall promptly update Customer with the information in this paragraph as soon as it becomes available.

6.3 Customer may require that Supplier's Processing of Customer Data be suspended, connectivity with Customer be terminated, or other appropriate action be taken pending such resolution.

6.4 Supplier agrees to keep Customer informed of progress and actions taken to address the Security Incident and prevention of future such Security Incidents, and to provide Customer with all facts about the Security Incident as appropriate for Customer to conduct its own assessment of the risk to Customer Data and of Customer's overall exposure to such Security Incident.

6.5 Unless such disclosure is mandated by law, Customer in its sole discretion will determine whether to provide notification to Customer's customers or employees concerning incidents involving Customer Data.

6.6 Notwithstanding any other provisions of this DPA or a Statement of Work, in the event of a Security Incident involving unencrypted Personal Data, Supplier agrees to provide the following at Supplier's expense upon Customer's request: (a) notice to individuals whose Personal Data was affected by the Security Incident in a manner and format determined by Customer, in its sole discretion, as well as to any other third parties, such as regulatory, law enforcement, or consumer reporting agencies, that Customer determines should be notified of the Security Incident, in its sole discretion, (b) one year of credit monitoring, (c) any other relief service(s) as required by applicable law to affected individuals; and (d) reasonable co-operation with Customer to offer any other remediation services deemed necessary by Customer or which are customarily provided to individuals impacted by a breach in confidentiality of their Personal Data in the relevant jurisdictions.

7 Insurance

To the extent Supplier does not already have in place insurance required by the Agreement that covers the following, Supplier shall purchase and maintain cyber risk or similar insurance (i) covering liability arising out of any Security Incident; (ii) with limits of liability equalling at least £7,500,000 or $10,000,000 per claim. Such insurance shall comply with the other insurance requirements set forth in the Agreement, or if there are no such other requirements, the following:

Supplier at its sole cost and expense shall maintain in full force and effect during the term of this DPA, with insurance companies having an A.M. Best's rating (or its equivalent) of A-VII or better, the above coverages. Supplier shall maintain such coverage or exercise an extended reporting period for at least three years after completion or termination of the Services. All insurance policies shall provide for, or Supplier shall provide, thirty (30) days' prior written notice to Customer in the event of

cancellation of any of the above-required policies. If required by Customer, Supplier shall provide to Customer satisfactory certificates of insurance evidencing the coverage required herein including all applicable endorsements. Customer's failure to request such certificates shall not constitute a waiver of Supplier's obligation to maintain the required minimum insurance. The required minimum limits of coverage set out above will not in any way restrict or serve to diminish Supplier's liability under this DPA.

ATTACHMENT 3

Module Two (Transfer Controller to Processor) of the EU 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) ([2]) for the transfer of 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

[2] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(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

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

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.

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 ([3]) (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;

[3] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(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

(a) OPTION 2: GENERAL WRITTEN AUTHORISATION 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 sixty (60) 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. ([4]) 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

(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

[4] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

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.

(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

(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

(a) Where the data exporter is established in an EU Member State: 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.

Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679: The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, 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

(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 ([5]);

(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

[5] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

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

OPTION 2: These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland (specify Member State).

Clause 18

Choice of forum and jurisdiction

(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 (*specify Member State*).

(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

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): All affiliates of Customer operating in the countries which comprise the European Economic Area, Switzerland, the United Kingdom and/or in any other country which accepts the EU Standard Contractual Clauses, which are controllers and which transfer personal data to the data importer.

Contact person's name, position and contact details: Marsh McLennan Privacy, privacy@mmc.com

Activities relevant to the data transferred under these Clauses:

As set out in the Principal Agreement.

Signature and date: Signed as of the Effective Date by virtue of issuing the purchase order to Supplier to which the Principal Agreement is attached.

Role (controller/processor): Controller

Data importer(s):

Name: The provider of the Services identified in the Principal Agreement

Address: As set out in the the Principal Agreement.

Contact person's name, position and contact details: As set out in the Principal Agreement.

Activities relevant to the data transferred under these Clauses:

As set out in the Principal Agreement.

Signature and date: Signed as of the Effective Date by virtue of providing Services in accordance with the purchase order to which the Principal Agreement is attached.

Role (controller/processor): Processor

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred
Customer and its Affiliates' personnel together with any other categories of data subjects contemplated by the Principal Agreement.

Categories of personal data transferred

Business contact information together with other categories of data contemplated by the Principal Agreement.

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.

None unless contemplated by the Principal Agreement.

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

Continuous basis as necessary to provide the Services.

Nature of the processing

As contemplated by the Principal Agreement.

Purpose(s) of the data transfer and further processing

For the purpose of providing and receiving the Services as set out in the Principal Agreement.

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

As necessary to provide the Services and as set out in this Exhibit.

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

[***To be completed, reflecting Attachment 1***]

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The supervisory authority of the EU Member State in which the data exporter is established.

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

(a) Organisational and technical measures designed to ensure that Customer Data is not Processed by Supplier or its Subcontractors for any purposes other than for the performance of the Services under the Agreement.

(b) Periodically updated inventories of (a) Personal Data that Supplier Processes and (b) Supplier systems that process Personal Data.

(c) Logical access controls to manage access to Customer Data and system functionality on a least privilege and need-to-know basis, including through the use of defined authority levels and job functions, unique IDs and passwords, Multi-factor Authentication or equally protective Risk-Based Authentication for system administrators and any remote access to its network and internal systems, and promptly revoking or changing access in response to terminations or changes in job functions.

(d) Password controls to manage and control password complexity, expiration and usage for all user accounts associated with access to Customer Data, whether directly or indirectly, including blocking user access after multiple unsuccessful password attempts and terminating sessions after a predetermined period of inactivity. Any password controlling access to Customer Data must be at least 8 characters in length, including a reasonable level of complexity, and a maximum expiration threshold of ninety (90) days.

(e) Customer Data is logically or physically segregated from any other data of Supplier or its customers.

(f) Physical controls to protect information assets from environmental hazards and unauthorised access, and to manage and monitor movement of persons into and out of Supplier's facilities where Customer Data is stored, processed, or transmitted.

(g) Operational procedures and controls to ensure technology and information systems are configured and maintained according to prescribed internal standards.

(h) Application security and software development controls designed to prevent the introduction of security vulnerabilities in any software developed by Supplier.

(i) Network security controls, including the use of firewalls, layered DMZs, and updated intrusion detection/prevention systems to help protect systems from intrusion and limit the scope or success of any attack or attempt at unauthorised access to Customer Data.

(j) Vulnerability management and regular application, operating system and other infrastructure scanning and patching procedures and technologies to identify, assess,

mitigate and protect against new and existing security vulnerabilities and threats, including viruses, bots, and other malicious code.

(k) Encryption of Customer Data in accordance with the requirements as set forth in Section 3 Data Protection of these Security Terms and using appropriate algorithms and key lengths to reasonably protect Customer Data against unauthorised access, disclosure, or theft.

(l) Business resiliency/continuity and disaster recovery procedures to ensure Supplier's ability to maintain service and recover from foreseeable emergency situations or disasters in a timely manner.

(m) Change management procedures to ensure all modifications to Supplier's technology and information assets are properly tested, approved, recorded, and monitored.

(n) Incident management procedures to allow for the proper investigation, response, mitigation and notification of events related to the confidentiality, integrity, and availability of Supplier's technology and information assets.

(o) Organisational management to ensure the proper development and maintenance of information security and technology policies, procedures and standards.

(p) Background checks (including criminal background checks) of any Personnel who may gain access to Customer Data that are repeated at adequate intervals, and administrative controls to ensure no one convicted of a crime of dishonesty, breach of trust, or money laundering is permitted to access Customer Data.

(q) Ensure no individual who has been convicted of a crime of dishonesty, breach of trust, or money laundering has access to Personal Data.

(r) Use of secure destruction procedures following NIST Media Sanitization standards (NIST 800-88 current revision) to sanitise any unencrypted hard disk, portable storage device or backup media containing Customer Data prior to sending it offsite for maintenance or disposal purposes.

ATTACHMENT 4

UK Addendum to the EU Standard Contractual Clauses

Except where otherwise defined in the DPA, capitalised terms used in this Annex have the meaning given to them in the Mandatory Clauses (as defined in Part 2 below in the table below).

In the event of a Restricted Transfer, the parties enter into this Addendum as issued by the ICO and as amended from time to time to the extent necessary to operate to provide Appropriate Safeguards for Restricted Transfers in accordance with Article 46 of the UK GDPR.

PART 1: TABLES	
TABLE 1	
PARTIES	The Parties are set out in Annex I A. of the Appendix to the Approved EU SCCs.
TABLE 2	
SELECTED SCCS, MODULES AND SELECTED CLAUSES	The version of the Approved EU SCCs shall be the version of the EU SCCs included at Attachment 3 to this DPA.

TABLE 3	
APPENDIX INFORMATION	Annex 1A: List of Parties: See the details for the data exporters and data importer(s) provided at Annex I A. to the Appendix of the version of the Approved EU SCCs.
	Annex 1B: Description of Transfer: See the description of transfer provided at Annex I B. of the Appendix to the Approved EU SCCs.
	Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II of the Appendix to the Approved EU SCCs.
	Annex III: List of Sub processors: Sub processors shall be engaged pursuant to Section 6 of this DPA and Clause 9 of the Approved EU SCCs.
TABLE 4	
ENDING THIS ADDENDUM WHEN THE APPROVED ADDENDUM CHANGES	Neither Party shall have the right to end this Addendum pursuant to Section 19.
PART 2: MANDATORY CLAUSES	
Mandatory Clauses of the Approved Addendum, being the template Addendum B.1.0 issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18 of those Mandatory Clauses	

ATTACHMENT 5

Switzerland Addendum to the EU Standard Contractual Clauses

Where the Standard Contractual Clauses apply to a transfer of Personal Data to which the FADP applies, the Standard Contractual Clauses shall be deemed to be amended to the extent necessary to operate to provide appropriate safeguards for such transfers in accordance with the FADP, including without limitation the following:

(i) Clause 13(a) and Part C of Annex I are not used; the "competent supervisory authority" is the Federal Data Protection and Information Commissioner;

(ii) the term "Member State" cannot be interpreted to exclude data subjects in Switzerland from exercising their rights under Data Protection Law;

(iii) the term "personal data" shall be deemed to include the data of legal entities to the extent such data is protected under the FADP; and

(iv) any amendments required from time to time by the Federal Data Protection and Information Commissioner in order to comply with the FADP.

ATTACHMENT 6

Transfer Requirements for Other Jurisdictions

Additional requirements to be added if needed.