Data Processing Terms and Conditions

("DPA Terms and Conditions")

1. APPLICABILITY

1.1. These DPA Terms and Conditions are concluded between the parties to a purchase order (subject to the Purchase Order Terms and Conditions) or a comprehensive agreement.

1.2. For all intents and purposes, (the "Controller") shall refer to the MultiChoice entity, including its Affiliates, while reference to (the "Processor") shall refer to the third party as set out in the Agreement (as defined below). For purposes of these DPA Terms and Conditions, each of the Controller and Processor shall inform the other in writing, of its data protection officer or the person holding a comparable role within such organisation.

1.3. Save as where the parties have executed a written data processing agreement, these DPA Terms and Conditions shall govern the relationship between the parties as far as Personal Data (as defined below) is Processed (as defined below).

2. DEFINITIONS AND INTERPRETATION

2.1. These DPA Terms and Conditions have been drafted for the benefit of the parties, and accordingly, the rule of construction that the contract shall be interpreted against or to the disadvantage of the party responsible for the drafting or preparation of these DPA Terms and Conditions (i.e., the *contra proferentem rule*), shall not apply.

2.2. Definitions, parties and agreement

2.2.1. **Definitions**. In these DPA Terms and Conditions, the following terms shall have the following meanings ascribed thereto:

2.2.1.1. "**Affiliates**" shall mean all the following entities from the Controller's group of companies including but not limited to: MultiChoice South Africa (Pty) Limited; MultiChoice Support Services (Pty) Limited; MultiChoice Africa Holdings BV, SuperSport International; (Pty) Ltd, DStv Media Sales (Pty) Ltd and Showmax s.r.o.

2.2.1.2. "**Agreement**" means a purchase order and/or written agreement entered into between the Controller and the Processor for the provision of the Services.

2.2.1.3. "**Applicable Data Protection Law/s**" means (subject to the provisions of clause 3) relevant data privacy and data protection legislation, regulations and binding

directives and/or codes applicable to the Processing carried out in relation to the Agreement and these DPA Terms and Conditions, and any other laws agreed between the parties in writing. For the avoidance of doubt, this includes (without limitation) any and all relevant data privacy and data protection legislation of the country where the Services are provided.

2.2.1.4. **"Data Subject"** is any identified or identifiable living human being, and includes in some instances, juristic persons for Applicable Data Protection Laws, to whom Personal Data relates.

2.2.1.5. "**EEA**" means the European Economic Area consists of the member states of the European Union.

2.2.1.6. "**Effective Date**" means the earlier of the date on which these DPA Terms and Conditions is signed by the Party last signing.

2.2.1.7. "**EU Standard Contractual Clauses**" means the Standard Contractual Clauses for data transfers outside the EEA adopted by the European Commission, in the extent of applicable modules, as attached in Annexure 4 to these DPA Terms and Conditions.

2.2.1.8. "**GDPR**" means the 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, and repealing Directive 95/46/EC (General Data Protection Regulation), as amended or replaced in the future.

2.2.1.9. "**Parties**" in these DPA Terms and Conditions:

2.2.1.9.1. the "**Controller**", as specified in the Agreement, is the person or entity who determines the scope of Personal Data (categories of data), the purpose of Processing ("why") and the means ("how") of Processing the Personal Data, and where the term is used, it will have the same meaning for the corresponding and/or similar term used in Applicable Data Protection Laws; and

2.2.1.9.2. the "**Processor**" is the processor, as specified in the Agreement and means the person or entity who:

2.2.1.9.2.1. Processes Personal Data on behalf of the Controller for the purpose of delivering the Services in terms of the Agreement and these DPA Terms and Conditions; and

2.2.1.9.2.2. and enters into these DPA Terms and Conditions with the Controller,

and where the term is used, it will have the same meaning for the corresponding and/or similar term used in Applicable Data Protection Laws.

2.2.1.10. **"Personal Data"** or **"Personal Information"** means any information about a Data Subject which is capable of directly or indirectly identifying them based on that information.

2.2.1.11. **"Personal Data Breach**" means the accidental, unauthorised or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, the Personal Data and where applicable under Applicable Data Protection Laws, shall where there are reasonable grounds to believe that any Personal Data has been accessed or acquired by an unauthorised person.

2.2.1.12. "**Personnel**" means any:

2.2.1.12.1. director, employee, or other person who works (permanently or temporarily) under the Processor's supervision; or

2.2.1.12.2. or person who renders services to the Processor for purposes of the Processor's obligations under these DPA Terms and Conditions, as their agent, consultant, contractor, or other representative.

2.2.1.13. **"Processing" or/"Process"** means any operation or set of operations which is performed on Personal Data, including but not limited to gathering, receipt, recording, processing, organising, collating, structuring, manipulation, adaptation or alteration, analysis, storage, erasure, disclosing, or disclosure by transmission; dissemination or otherwise making available; retrieval; consultation; use; alignment or combination, or combining with other information, restriction; anonymising or anonymisation or de-identifying; encryption or encrypting; and destruction.

2.2.1.14. "**Sensitive Personal Data**" **or** "**Sensitive Personal Information**" means Personal Data revealing racial or ethnic origin, political persuasion or opinions, religious or philosophical beliefs, trade union membership, genetic data or biometric data, data concerning health or sex life, or data relating to criminal behaviour and/or criminal convictions and offences or data of children.

2.2.1.15. "**Services**" means the services which the Processor is appointed to provide to the Controller in accordance with the Agreement and which require Processing of Personal Data on behalf of the Controller.

2.2.1.16. **"Sub-processor"** means any downstream processor that the Processor engages to process Personal Data in accordance with the Agreement and these DPA Terms and Conditions, with such sub-processor being pre-approved by the Controller in accordance with the terms of the Agreement and these DPA Terms and Conditions.

2.2.1.17. "**Supervisory Authority**" means the relevant data protection authority or regulator which is competent with respect to the relevant Processing under the Applicable Data Protection Law.

2.2.1.18. "**Third Country**" shall mean the following: (i) for transfers of Personal Data from the EEA, it shall mean any country outside the EEA for which there is no applicable adequacy decision adopted by the European Commission; or (ii) for transfers of Personal Data outside the United Kingdom, it shall mean any country, except for the EEA countries, the countries for which there is an applicable adequacy decision adopted by the European Commission and the countries for which there is an applicable adequacy regulation adopted by the government of United Kingdom or (iii) shall mean the country wherein Personal Data is transferred outside of the country wherein the Applicable Data Protection Law applies.

2.2.1.19. "**UK GDPR**" means the GDPR, as amended by Schedule 1 to the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 (SI 2019/419), as amended or replaced in the future.

2.2.1.20. "**UK Standard Contractual Clauses**" means Standard Contractual Clauses for transfers of personal data to controllers adopted by the European Commission under the decision 2001/497/EC and Standard Contractual Clauses for transfers of personal data to processors adopted by the European Commission under the decision 2010/87/EU, as adapted by the supervisory authority of the United Kingdom, the Information Commissioner's Office.

2.3. **Agreement**: The DPA Terms and Conditions are concluded in conjunction with the Agreement. In the event of a contradiction between the terms of these DPA Terms and Conditions and the provisions of the agreement, the terms of these DPA Terms and Conditions shall prevail. The DPA Terms and Conditions and its annexures shall be interpreted in the following order of precedence:

(1) Annexure 4: EU Standard Contractual Clauses and UK Standard Contractual Clauses, as referred to in clauses 11 of the DPA Terms and Conditions, (2) Annexure 1: Details of Processing,

(3) main body of the DPA Terms and Conditions, (4) Annexure 3: Technical and Organisational Measures and (5) Annexure 2: Authorized Sub-processors. This notwithstanding, the terms of these DPA Terms and Conditions shall not be interpreted in such a way that they conflict with any rights and obligations provided for under Applicable Data Protection Laws.

3. Controller's Instructions and Applicable Data Protection Law

3.1. In the course of providing the Services to the Controller and pursuant to the Agreement, the Processor has a requirement to access and Process certain Personal Data. Therefore, the Controller allows the Processor to Process the Personal Data, as further specified herein, on its behalf and strictly in accordance with:

3.1.1. the instructions of the Controller set forth herein and in terms of such further documented instructions that the Controller may issue at its discretion at any time; and

3.1.2. the terms of these DPA Terms and Conditions.

3.2. The Processor shall only Process the types of Personal Data relating to the categories of Data Subjects and for the specific purposes set out in the Annexure 1 hereto and shall not Process Personal Data to any third party other than in accordance with the Controller's documented instructions.

3.3. For the avoidance of doubt the Parties agree that the Processor is not authorised to Process the Personal Data for any other purposes than those specified in these DPA Terms and Conditions, and in particular, may not Process the Personal Data for the Processor's own purposes, unless required by applicable law, in accordance with clause 3.4 below.

3.4. Should the Processor be required to Process the Personal Data in compliance with any law (including any Applicable Data Protection Law/s), the Processor shall inform the Controller in writing of such requirement before the commencement of the Processing unless the law prohibits this on the grounds of public interest. In such case, the Processor shall inform the Controller as soon as possible.

3.5. The Processor shall ensure full and continuous compliance with all relevant provisions of the Applicable Data Protection Laws which apply to the Processing in question. Where the data protection law in the country in which such Processing takes place is either –

3.5.1. not equivalent to the GDPR; or

3.5.2. such country does not have any local data protection laws in force and effect,

then the provisions of the GDPR shall take precedence for purposes of these DPA Terms and Conditions, provided that in the case where clause 3.5.1 is applicable, the Processor shall continue to remain responsible for full compliance with the specific provisions of the Applicable Data Protection Law, particularly where the requirements are additional to those set out in the GDPR.

3.6. The Processor is obliged to immediately notify the Controller in writing in the event it can no longer ensure compliance with applicable law(s), including Applicable Data Protection Laws.

3.7. If the Controller issues an instruction that infringes Applicable Data Protection Laws, the Processor shall immediately notify the Controller in writing of such claimed infringement, following which the Controller shall (i) provide a written response as to its reason for its opinion that the instruction does not infringe Applicable Data Protection Laws (including the legal soundness of the instruction); or (ii) amend the initial instruction provided to the Processor to ensure compliance with the Applicable Data Protection Laws. The Processor may terminate these DPA Terms and Conditions on 1 (one) month's written notice to the Controller following the response by the Controller in response to the Processor's notification referred to in this clause 3.7 should the response reasonably and legally fail to provide legally sound reasoning, and thus infringes the Applicable Data Protection Laws.

3.8. To the extent that any Personal Data is Processed by the Processor outside of the country in which the Controller has made the Personal Data available to the Processor and/or in which the Controller itself Processes such Personal Data, the Processor shall ensure that technical and organisational measures for cross border data transfers under Applicable Data Protection Laws are put in place and adhered to.

3.9. To the extent that the Processing includes Processing of Data Subjects Sensitive Personal Data, the Processor shall ensure that Applicable Data Protection Laws are adhered to in this Processing. Furthermore, it shall ensure that technical and organisational measures are put in place and adhered to.

4. Duration and Breach

4.1. The DPA Terms and Conditions shall be effective from the Effective Date (i) until the Services requiring Processing of Personal Data on behalf of the Controller are terminated; (ii) or until the termination or expiration of the Agreement, whichever is later.

4.2. If the Processor commits a material breach of any provision of these DPA Terms and Conditions, the Controller shall request in writing that the Processor remedy the breach within a period specified by the Controller. The Controller shall have the right, on failure by the Processor to remedy the breach, to cancel the Principal Agreement and this DPA Terms

and Conditions with immediate effect on further written notice to the Processor. A material breach of any provision of these DPA Terms and Conditions shall also be considered a material breach of the Agreement.

4.3. The Controller is also entitled to terminate the Agreement with immediate effect if (i) the Processor is in substantial or persistent breach of these DPA Terms and Conditions or its obligations under Applicable Data Protection Laws; or (ii) it fails to comply with a binding decision of a competent court or the Supervisory Authority/ies regarding its obligations under these DPA Terms and Conditions or Applicable Data Protection Laws.

4.4. The expiration or termination of these DPA Terms and Conditions shall not affect provisions of these DPA Terms and Conditions which are expressly provided to operate after any such expiration or termination, or which out of necessity must continue to have effect after such expiration or termination, notwithstanding that the relevant provisions themselves do not provide for this. Without derogating from or limiting the foregoing, this clause 4.4 and clauses 10,12 and 13 shall continue in full force and effect after expiration or termination of these DPA Terms and Conditions.

5. Security

5.1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, the Processor is required to implement appropriate technical and organisational measures to adequately protect the Personal Data against a Personal Data Breach and from any misuse and loss in accordance with the requirements of Applicable Data Protection Laws. In particular but not limited to, the Processor undertakes to implement, and require its Sub-processors to implement, the technical and organisational measures described in Annexure 3: Technical and Organisational Measures.

5.2. In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise Processed as well as any laws in the country in question where such processing involves cross border data transfers. Where required, the Processor shall comply with the additional security measures as requested by the Controller under documented instructions.

5.3. In addition to the obligations set out above, the Processor shall provide necessary assistance and information to the Controller for the following purposes:

5.3.1. carrying out a data protection impact assessment or inherent risk assessment where the Processing is likely to be considered a high risk to the rights and freedoms of the Data Subjects;

5.3.2. consulting the Supervisory Authority/ies prior to Processing where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk; and

5.3.3. ensuring that Personal Data is accurate and up to date, by informing the Controller without delay if the Processor becomes aware that the Personal Data it is Processing is inaccurate or has become outdated.

5.4. The Processor shall maintain a record of Processing activities that relate to the Processing of Personal Data on behalf of the Controller, as well as the record of associated risks. The Processor shall provide these records to the Controller upon its request.

5.5. The Processor shall conduct regular control checks concerning its and its Sub-processors' compliance with its obligations towards data protection and security hereunder.

6. The Processor's Personnel

6.1. The Processor shall take reasonable steps to ensure the reliability of any Personnel who may have access to the Personal Data, ensuring in each case that access is strictly limited to those individuals who need to access the Personal Data, as strictly necessary for performance of that person's duties in relation to the Services, and ensuring that all such individuals:

6.1.1. are informed of the confidential nature of the Personal Data and are aware of the Processor's obligations under these DPA Terms and Conditions in relation to the Controller Personal Data;

6.1.2. have undertaken appropriate training in relation to information security and privacy and in the Applicable Data Protection Laws;

6.1.3. are subject to confidentiality undertakings or professional or statutory obligations of confidentiality which shall continue for duration of 3 (three) years after the termination of the relevant person's access to the Personal Data; and

6.1.4. are subject to user authentication and log-on processes when accessing the Controller's Personal Data.

7. Sub-processing

7.1. Subject to clause 7.2, the Processor shall not engage any Sub-processors to process the Controller's Personal Data without the prior written approval of the Controller, which the Controller may refuse in its absolute discretion.

7.2. As of Effective Date of these DPA Terms and Conditions, the Controller hereby authorises the Processor to engage those Sub-processors set out in Annex 2 (Authorised Sub-processors). The Processor warrants that the contractual terms it concludes with the Sub-processors, set out in Annex 2, will in substance be the same as those the set out in these DPA Terms and Conditions. Upon request, the Processor shall provide a copy of its agreements with the Sub-processors to the Controller for its review.

7.3. The Processor shall ensure that the Controller has substantially the same control rights over each Sub-processor that the Processor engages as the Controller has over the Processor under these DPA Terms and Conditions. Further chaining of Sub-processors is not allowed without the Controller's written prior approval. If the Controller grants such approval, the same obligations shall apply to such further Sub-Sub-processors.

7.4. While the Processor shall remain fully responsible to the Controller for the performance of each Sub-processor under the Agreement, the Processor shall take steps to ensure that the Sub- processors each comply with the obligations to which the Processor is subject under these DPA Terms and Conditions and under Applicable Data Protection Laws.

8. Data Subject Rights and Supervisory Authority's Requests

8.1. The Processor shall promptly notify the Controller in writing if it receives a request from a Data Subject or any request, enquiry, notice, decision or other communication from any competent Supervisory Authority in respect of the Controller's Personal Data. It shall not respond to the request itself, unless authorised to do so by the Controller.

8.2. The Processor shall co-operate as requested by the Controller to enable the Controller to comply with any Data Subject's or Supervisory Authority's request under the Applicable Data Protection Laws in respect of the Controller's Personal Data or these DPA Terms and Conditions, which shall include:

8.2.1. the provision of all data requested by the Controller within any reasonable timescale specified by the Controller in each case, but in any case, not longer than three (3) days, including full details and copies of the request or complaint, communication or request, relating information and any of the Controller's Personal Data it holds in relation to the request;

8.2.2. where applicable, providing such assistance as is reasonably requested by the Controller to enable the Controller to comply with the relevant request within the timescales prescribed by the Applicable Data Protection Law or the competent Supervisory Authority; and

8.2.3. implementing any additional technical and organisational measures as may be reasonably required by the Controller to allow the Controller to respond effectively to relevant complaints, communications or requests.

8.3. The Processor shall assist the Controller by appropriate technical and organisational measures, with the fulfilment of the Controller's obligation to respond to requests for exercising a Data Subject's rights.

8.4. If the Processor receives any request for access to Controller's Personal Data from any government authority, the Processor shall strive to re-direct the relevant government authority to request access from the Controller. If this is not possible, the Processor shall notify the Controller immediately of the request. The Processor shall verify that the request for access is valid and legitimate and shall, in agreement with the Controller, use all available legal remedies to defend the Controller and refuse direct access to Controllers' Personal Data.

9. Personal Data Breach

9.1. The Processor shall notify the Controller promptly and where required under Applicable Data Protection Laws, immediately, and in any case within twenty-four (24) hours, upon becoming aware of or reasonably suspecting a Personal Data Breach involving the Data Subject(s) Personal Data, providing the Controller with sufficient information (including the identity of the person or persons known or suspected of being responsible for the Personal Data Breach) which allows the Controller to meet any obligations to report and to address and mitigate the impact of a Personal Data Breach under the Applicable Data Protection Law. Such notification shall as a minimum:

9.1.1. describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned, as well as information when the data breach occurred and when the Processor became aware thereof;

9.1.2. communicate the name and contact details of the Processor's Data Protection Officer or other relevant contact from whom more information may be obtained;

9.1.3. describe the likely consequences of the Personal Data Breach; and

9.1.4. describe the measures taken or proposed to be taken to address the Personal Data Breach and including where appropriate, describe measures to mitigate its possible adverse effects.

9.2. Where, and insofar as it is not possible for the Processor to provide the abovementioned information all at the same time, the initial notification to the Controller should contain the information then available and further information shall, as it becomes available, subsequently be provided to the Controller without undue delay.

9.3. Unless the Parties agree otherwise in writing, notification from the Processor to the Controller under this clause shall be made by e-mail with confirmation of receipt under the following e-mail address: DPO@multichoice.co.za.

9.4. The Processor shall co-operate with the Controller and take such reasonable commercial steps, such as but not limited to acquiring the services of an independent external party/ies, and/or acquiring additional security software, as are directed by the Controller to assist in the investigation, mitigation and remediation of each Personal Data Breach and for the Controller to comply with Applicable Data Protection Law requirements and in addition, the Processor shall fully comply with all obligations placed on the Processor in relation to addressing a Personal Data Breach under Applicable Data Protection Laws.

9.5. In the event of a Personal Data Breach, the Processor shall not inform any third party without first obtaining the Controller's prior written consent, unless notification is required by Applicable Data Protection Laws to which the Processor is subject, in which case the Processor shall to the extent permitted by such law inform the Controller of that legal requirement, provide a copy of the proposed notification and consider any comments made by the Controller before notifying the Personal Data Breach to the relevant Supervisory Authority.

9.6. Without prejudice to clause 9.1, the Processor shall, without undue delay, inform the Controller in case of a serious interruption of operations, suspicion of a Personal Breach, any breach of Applicable Data Protection Law or these DPA Terms and Conditions, and any other irregularity in Processing the Personal Data.

9.7. The Processor shall keep a record of all Personal Data Breaches, including information about the cause of the Personal Data Breach, its consequences and measures adopted to remedy and prevent the occurrence of the Personal Data breach in the future. The Processor shall provide the record to the Controller upon its request.

10. Deletion or Destruction, and/or return of the Personal Data

10.1. The Processor shall promptly and in any event within 60 (sixty) calendar days of the termination or expiry of the Principal Agreement and this DPA Terms and Conditions, at the choice of the Controller (such choice to be notified to the Processor in writing) either:

10.1.1. return all Personal Data to the Controller by secure file transfer in such format as notified by the Controller to the Processor and securely delete all other copies of the Personal Data Processed by Processor or any authorised Sub-processor; and/or

10.1.2. securely delete or destroy all Personal Data Processed by Processor or any authorised Sub-processor, and in each case provide written certification to the Controller that it has complied fully with this clause 10.

10.2. The Processor shall continue to ensure compliance with this DPA during the deletion or destruction.

11. Documentation and Audit rights

11.1. The Processor shall deal promptly and adequately with any inquiries from the Controller about the Processing under these DPA Terms and Conditions. The Processor shall make available to the Controller all information necessary to demonstrate compliance with these DPA Terms and Conditions and Applicable Data Protection Laws. At the Controller's request, the Processor shall also permit and contribute to audits of the Processing activities under these DPA Terms and Conditions, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the Controller may take into account relevant certifications held by the Processor.

11.2. The Controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the Processor and shall, where appropriate, be carried out with reasonable notice. The Processor shall grant access to such premises or facilities to the Controller or the independent auditor.

11.3. The Processor shall provide full co-operation to the Controller and the independent auditor, as applicable, in respect of any such audit and shall at the request of the Controller, provide the Controller with evidence of compliance with its obligations under these DPA Terms and Conditions.

11.4. The Parties shall make the information referred to in this clause, including the results of any audits, available to the Supervisory Authority/ies on request.

12. Transfers of the Controller Personal Data to Third Countries

12.1. If the Controller, as a data exporter, transfers Personal Data that is subject to the GDPR to the Processor, as a data importer, who is established in a Third Country, such transfer shall be subject to the EU Standard Contractual Clauses in the applicable extent, as set out in Annexure 4: EU Standard Contractual Clauses; the relevant information required by the Annexes of the EU Standard Contractual Clauses shall be provided in Annexures to these DPA Terms and Conditions.

12.2. If the Controller, as a data exporter, transfers Personal Data that is subject to the UK GDPR to the Processor, as a data importer, who is established in a Third Country, such transfer shall be subject to the relevant UK Standard Contractual Clauses in the minimum applicable extent, which are hereby incorporated in these DPA Terms and Conditions (for the avoidance of doubt, optional clauses shall not apply); the relevant information required by the Annexes of the EU Standard Contractual Clauses shall be provided in Annexures to these DPA Terms and Conditions.

12.3. The Parties acknowledge and agree that, subject to their mutual agreement, other appropriate safeguards for transfers of Personal Data to Third Countries may be applicable, subject to the applicable requirements of the GDPR and the UK GDPR or Applicable Data Protection Laws.

12.4. To the extent that any Personal Data is transferred by the Controller who is subject to any other Applicable Data Protection Laws, other than the GDPR and the UK GDPR, to the Processor located in another third country, the Controller acknowledges that it will be required to comply with the requirements applicable to cross-border data transfers under Applicable Data Protection Laws and shall ensure appropriate safeguards for cross border data transfers under Applicable Data Protection Laws.

12.5. Where any Applicable Data Protection Laws may require the approval of the Supervisory Authority for cross border transfer of Personal Data from that country to a third country or organisation, such transfer may only be undertaken by the Processor against it having obtained such approval.

12.6. The Parties undertake to negotiate and execute any other agreements or documents that might be adopted by competent public authorities for the purpose of amending, replacing, supplementing or superseding the EU Standard Contractual Clauses and/or the UK Standard Contractual Clauses, or for the purpose to fulfil any other requirements relating to transfers of Personal Data to Third Countries, as applicable.

12.7. Where the Processor engages a Sub-processor in Processing activities that involve a transfer (or an onward transfer) of Personal Data to a Third Country, the Processor shall

ensure that the Personal Data is Processed lawfully. Before the transfer to a Third Country, the Processor shall ensure that the Sub-processor has implemented appropriate technical and organisational measures which provide for adequate safeguards, in particular (without limitation), the Processor and the Sub- processor must comply with the requirements of Applicable Data Protection Laws and where applicable, shall execute the EU Standard Contractual Clauses or the UK Standard Contractual Clauses. The Processor shall ensure that these measures are also applied in case of any further onward transfers approved by the Controller.

13. Indemnity

13.1. The Processor shall indemnify and hold harmless the Controller against all damages, losses, fines, penalties and sanctions arising from any claim by a third party or Supervisory Authority arising from any breach of the terms of these DPA Terms and Conditions and Applicable Data Protection Laws, including any administrative fines that may be imposed by any relevant Supervisory Authority.

14. Communication

14.1. Unless otherwise agreed by the Parties, the contact details related to the day-to-day communication regarding the matters related to the performance of these DPA Terms and Conditions shall be as set out on the Agreement.

15. Miscellaneous

15.1. Neither the rights nor the obligations of any Party may be assigned in whole or in part without the prior written consent of the other Party, provided, however, that these DPA Terms and Conditions may be transferred or assigned on the terms and conditions set out in the Agreement.

15.2. Each Party shall remain responsible for its compliance and the compliance of all its employees, agents and third parties with the obligations under these DPA Terms and Conditions. Each Party shall make or obtain and maintain so long as it is a party to these DPA Terms and Conditions all necessary licenses or notifications which such party is obliged to obtain and maintain pursuant to Applicable Data Protection Laws.

15.3. In the event of any dispute arising between the Parties in connection with these DPA Terms and Conditions, the Parties shall negotiate in good faith to resolve their dispute. If the dispute cannot be resolved by good faith negotiations by the Parties, the dispute shall be finally settled by competent courts having jurisdiction to hear the matter as noted in the Agreement.

15.4. Unless the standard contractual clauses as per the GDPR require a different applicable law to apply (in which case such law will be governing law of these DPA Terms and Conditions), these DPA Terms and Conditions are governed by laws of the country where the Services are being provided.

15.5. Should any provision of these DPA Terms and Conditions be invalid or unenforceable, then the remainder of these DPA Terms and Conditions shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible,

15.6. (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

Annexure 1: DETAILS OF PROCESSING OF THE CONTROLLER PERSONAL DATA

This Annexure 1 includes certain details of the Processing of the Controller's Personal Data as required by Applicable Data Protection Laws.

Subject matter and duration of the Processing of the Personal Data

The subject matter of the Processing is to provide Services under the Agreement and duration of the Processing of the Personal Data is set out in the Agreement and the DPA Terms and Conditions.

Nature and purpose of the Processing of the Controller Personal Data

The nature and the purpose of Processing corresponds to the provision of Services, as set out in the Agreement.

Categories of the Personal Data to be Processed by the Processor

Subject to confirmation otherwise by the Controller, the following categories of Personal Data are generally processed by the Processor:

- Name and surname
- Email address
- Residence address
- IP address
- Phone number
- Usage data
- Job position
- Date of birth

Sensitive data Processed (if applicable) and applied restrictions or safeguards - ……..

Categories of Data Subjects to whom the Controller's Personal Data relates
Subject to confirmation otherwise by the Controller, the Personal Data will relate to the following categories of Data Subjects generally processed by the Processor:

- Employees
- Suppliers
- Customers
- Prospects
- Consultants
- Visitors
- Contractors Other:

Frequency of the transfer outside the EEA

Subject to confirmation otherwise by the Controller, transfers of Personal Data shall be

- One-off
- Continuous basis

Retention period

For the duration of the provision of the Processor's Services to the Controller and in accordance with applicable Agreement between the Controller and the Processor.

For transfers to Sub-processors, also specify subject matter, nature and duration of the Processing

Subject matter and nature – provision of services, to be notified in writing to the Controller, using the substantively the same format as set out in Annexure 2

Duration – duration of the provision of Sub-processor's services.

The obligations and rights of the Controller

The obligations and rights of the Controller are set out in these DPA Terms and Conditions.

Annexure 2: AUTHORISED SUBPROCESSORS

Full Registered Name and Registered Office	Contact Person	Contact Details	Location of Processing	Description of Processing activities

The Processor undertakes to submit the information relating to its proposed Sub-Processors to the Controller for authorisation, using this substantively the same format set out in this Annexure 2.

Annexure 3: TECHNICAL AND ORGANISATIONAL MEASURES

The Processor undertakes to implement, and require its Sub-processors to implement, the following technical and organisational measures:

a) the ability to ensure the ongoing security, confidentiality, integrity, availability and resilience of processing systems, networks and services;
b) the ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident;
c) a process for regularly monitoring, testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the Processing;
d) prevention of unauthorised persons' gaining access to data processing systems (physical access control);
e) prevention of data processing systems being used without authorisation (logical access control);
f) keeping Personal Data logically separate from data Processed on behalf of any third party;
g) applying encryption and pseudonymisation of the Personal Data, where appropriate;
h) ensuring that in the course of Processing or use and after storage, Personal Data cannot be read, copied, modified or deleted without authorisation (data access control);
i) ensuring that the Personal Data cannot be read, copied, modified or deleted without authorisation during electronic transmission, transport or storage, and that the target entities for any transfer of the Personal Data by means of data transmission facilities can be established and verified (data transfer control);
j) ensuring the establishment of logging and an audit trail to document whether and by whom the Personal Data have been entered into, modified in, or removed from data processing systems (entry control);
k) maintaining an information security policy and security incident management and continuity plans, consisting of, among others, the analysis performed in this respect and the risk management of personal data, a description of various responsibilities and organizational rules, description of how security incidents are managed, the measure that were introduced to keep the security system up-to-date after installation;
l) organising information security by means of selection of an information security lead who has the necessary competences, is adequately trained, ensures that various responsibilities with regard to information security have been clearly laid out, ensures that the responsibilities defined in the information policy are performed and who cannot discharge any function nor take up any responsibility that is incompatible with the information security governance role;

m) ensuring physical environment security, for instance by means of security and surveillance regarding building, premises and installations where carriers of personal data and computer systems processing the data are positioned, as well as prevention, detection and operating procedure in the case of fire, intrusion and water damage;

n) maintaining complete and up-to-date documentation proportionate to the risk profile of the processing operations, including, but no limited to, technical documentation of implemented security measures and other information necessary to demonstrate compliance with the requirements of these DPA Terms and Conditions; and

o) ensuring that the Personal Data is Processed solely in accordance with the relevant Controller's instructions (control of instructions)

Annexure 4: EU STANDARD CONTRACTUAL CLAUSES – MODULE 2 (TRANSFER CONTROLLER TO PROCESSOR)

These EU Standard Contractual Clauses are entered into between MultiChoice (the Controller, as defined in the DPA Terms and Conditions) and the Vendor (the Processor, as defined in the DPA Terms and Conditions).

WHEREAS:

(A) MultiChoice procures certain Services and outsources certain processing activities to Vendor based on the Agreement which requires Processing of Personal Data. MultiChoice primarily acts as the Controller and the Vendor primarily acts as the Processor and the parties have entered into the DPA Terms and Conditions governing the Processing of MultiChoice's Personal Data by Vendor on behalf of MultiChoice.

(B) Subject to the configuration of Services provided by the Vendor, Vendor may Process Personal Data as a Controller. In the event that (i) the Personal Data is subject to the GDPR, (ii) MultiChoice Processes Personal Data as a Controller and the Vendor Processes Personal Data as a Controller and (iii) the Processing requires a transfer from the EEA to a Third Country or an onward transfer to a Third Country, as defined in the DPA Terms and Conditions, any such transfer of Personal Data shall be subject to these EU Standard Contractual Clauses in the extent: **MODULE TWO: Transfer Controller to Processor**.

Sections marked as "**MODULE ONE: Transfer Controller to Controller**", "**MODULE THREE: Transfer Processor to Processor**" and sections marked as "**MODULE FOUR: Transfer Processor to Controller**" shall not apply. For the avoidance of doubt, if applicable, the Parties shall enter into separate EU Standard Contractual Clauses with respect to Module One, Module Three and Module Four.

(C) These EU Standard Contractual Clauses are incorporated into the DPA Terms and Conditions executed between the Parties that shall govern the matters not settled by these EU Standard Contractual Clauses. These Standard Contractual Clauses shall have control over the DPA Terms and Conditions and any other agreements entered into between the Parties with respect to Processing of Personal Data. For the avoidance of doubt, if several EU Standard Contractual Clauses are applicable in the extent of applicable modules, none of them shall control over the other.

(D) These EU Standard Contractual Clauses shall become effective as of the Effective Date of the DPA Terms and Conditions and shall replace and supersede any already existing standard contractual clauses concluded between the Parties in the scope set forth in section (B) above.

(E) Capitalized terms used and not defined in these EU Standard Contractual Clauses have the meaning given to them in the DPA Terms and Conditions or, as applicable, the GDPR.

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) 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 set out in the DPA Terms and Conditions to which this Annexure 5 is attached (hereinafter the '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, set out in the DPA Terms and Conditions to which this Annexure 5 is attached (hereinafter the 'data importer')

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

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8.1(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 the DPA Terms and Conditions concluded between the Parties, 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 and/or in the DPA Terms and Conditions. *Clause 7*

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 and in the DPA Terms and Conditions, 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 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 and/or in the DPA Terms and Conditions. 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 and in the DPA Terms and Conditions. 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 (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 30 (thirty) days prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

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

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

Clause 11

Redress

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

(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.

(b) 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.

(c) 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) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679, the supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(d) 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;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

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

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

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 the Netherlands

(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.

ANNEX I

A. LIST OF PARTIES – refer to the Agreement

B. DESCRIPTION OF TRANSFER

Refer to Annexure 1 of the DPA Terms and Conditions for details.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority in accordance with Clause 13 is the Dutch Data Protection Authority (Dutch supervisory authority).

ANNEX II

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

Refer to the DPA Terms and Conditions for details

The technical and organisational security measures are set out in Annexure 3 of the DPA Terms and Conditions and as may communicated in writing by the data exporter to the data importer from time to time.

ANNEX III

LIST OF SUB-PROCESSORS

The Processor undertakes to submit the information relating to its proposed Sub-Processors to the Controller for authorisation, using this substantively the same format set out in Annexure 2. See Annexure 2 of the DPA Terms and Conditions.