CULTURE EXCELLENCE DATA PROCESSING AGREEMENT (DPA) (END-CUSTOMER) VERSION 1.1

STANDARD CONTRACTUAL CLAUSES FOR INTERNATIONAL TRANSFERS AND THE PROCESSING OF PERSONAL DATA

This forms an agreement between Culture Excellence ("**CE**" or "**data importer**") and the end-customer of CE ("**End-customer**" or "**data exporter**") (individually referred as the "**Party**" and jointly referred as the "**Parties**") and enters into force along with the Parties' conclusion of a commercial agreement and/or with the End-Customer's acknowledgement of the CE Culture Excellence Terms and Conditions regarding CE's deliveries of services to the End-customer and/or with signature of this DPA. The parties may have been engaged by a third party sales partner (refer to CE's website for sales partner information), however, the sales partner does not assume a data processing role under this agreement.

The agreement includes both the EU Commissions Standard Contractual Clauses for International Transfers (governing transfers from EU/EEA) as well as the supplementary UK International Data Transfer Addendum to the European Commission's Standard Contractual Clauses for International Transfers (governing transfers from UK as supplement to the EU version).

As to allocation of roles regarding the transfers to/from End-customer/CE and the processing of personal data, the below describes this allocation of roles and the respective situations, which is governed by and decribed in detail in the EU Commissions Standard Contractual Clauses for International Transfers and the UK International Data Transfer Addendum below:

- **MODULE ONE: Transfer controller to controller:** governs transfers outside the scope of MODULE TWO (described below) and, thus, solely relates to information in the relation between the End-customer and CE outside the scope of the data processor constellation.
- **MODULE TWO: Transfer controller to processor:** governs the situation where an End-customer (the data controller) purchases the Culture Excellence Program directly from CE (acting as data processor), due to the Processing of Personal Data in the survey tool based on the instruction from the End-customer purchasing the Culture Excellence Program. This is the main rule for any data Processing activity under this agreement.

SECTION I

Clause 1

Purpose and scope

(a) The Purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of Personal Data to a third country.

[1] 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 of 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)

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the Personal Data, as listed in Annex I.A. (hereinafter each "data exporter"), and

(ii) the entity/ies in a third country receiving the Personal Data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

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

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

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

Clause 2

Effect and invariability of the Clauses

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

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

Clause 3

Third-Party beneficiaries

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

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

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

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

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

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

Clause 4

Interpretation

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 […].

(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.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall Process the Personal Data only for the specific Purpose(s) of the transfer, as set out in Annex I.B. It may only Process the Personal Data for another Purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of Personal Data Processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the Personal Data to any third Party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the Purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including Personal Data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the Personal Data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that Personal Data that is inaccurate, having regard to the Purpose(s) of Processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the Personal Data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the Personal Data is adequate, relevant and limited to what is necessary in relation to the Purpose(s) of Processing.

8.4 Storage limitation

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

8.5 Security of Processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the Personal Data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "Personal Data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and Purpose(s) of Processing and the risks involved in the Processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the Purpose of Processing can be fulfilled in that manner.

[2] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to Process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a Personal Data breach concerning Personal Data Processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the Personal Data breach, including measures to mitigate its possible adverse effects.

(e) In case of a Personal Data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and Personal Data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a Personal Data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the Personal Data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the Personal Data breach.

(g) The data importer shall document all relevant facts relating to the Personal Data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

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

8.7 Onward transfers

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

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

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

[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.

(iii) the third Party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

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

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(1) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its Purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

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

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the Processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(c) 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.

(d) 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

(e) 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.

(f) 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.

(g) 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.

(h) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely

identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

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

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

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

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

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

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

[4] 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.

Clause 9

Use of sub-processors

MODULE TWO: Transfer controller to processor

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 one month 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.

(i) 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.[5] 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.

(j) 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.

(k) 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.

(l) 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.

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

Clause 10

Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the Processing of his/her Personal Data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[6] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge :

(i) provide confirmation to the data subject as to whether Personal Data concerning him/her is being Processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if Personal Data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the Personal Data has been or will be onward transferred, the Purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase Personal Data concerning the data subject if such data is being or has been Processed in violation of any of these Clauses ensuring third-Party beneficiary rights, or if the data subject withdraws the consent on which the Processing is based.

(c) Where the data importer Processes the Personal Data for direct marketing Purposes, it shall cease Processing for such Purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated Processing of the Personal Data transferred (hereinafter "automated decision"), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

[6] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(h) 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.

(i) 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.

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

Clause 11

Redress

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-Party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

MODULE ONE: Transfer controller to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-Party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-Party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-Party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(a) *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.

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.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures.

It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

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

Clause 14

Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the Processing of the Personal Data by the data importer, including any requirements to disclose Personal Data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the Processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the Purpose of Processing; the categories and format of the transferred Personal Data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[7];

(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.

[7] 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.

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

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

Clause 15

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of Personal Data transferred pursuant to these Clauses; such notification shall include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

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

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the Personal Data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of Personal Data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the Processing of Personal Data under these Clauses, where:

(i) the data exporter has suspended the transfer of Personal Data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

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

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

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of Personal Data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the Personal Data is transferred. This is without prejudice to other obligations applying to the Processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-Party beneficiary rights. The Parties agree that this shall be the law of the Member State where the End-customer is established.

Clause 18

Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the Member State where the End-customer is established.

(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 1 – DETAILS OF THE PROCESSING OF PERSONAL DATA

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

Data exporter(s):

Name: The End-customer

Address: Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture Excellence Terms and Conditions and/or the details provided on the signature page of this DPA.

Contact person's name, position and contact details: Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture Excellence Terms and Conditions and/or the details provided on the signature page of this DPA.

Activities relevant to the data transferred under these Clauses: To enable the Processing of and transfer of Personal Data on behalf of the End-customer.

Signature and date: enters into force along with the Parties' conclusion of a commercial agreement and/or with acknowledgement by the End-Customer of CE's Culture Excellence Terms and Conditions regarding CE's deliveries of services to the End-customer and/or with signature of this DPA.

Role (controller/processor): controller and processor (see below).

Data importer(s):

1. Name: Culture Excellence

Address: DSO-DDP-A5-D-FLEX-G001, Building A5, Dubai Silicon Oasis, Dubai, UAE.

Contact person's name, position and contact details: David Shannon (Owner); dave@culturexcellence.com.

Activities relevant to the data transferred under these Clauses: To enable the Processing of and transfer of Personal Data on behalf of the End-customer.

Signature and date: enters into force along with the Parties' conclusion of a commercial agreement and/or with acknowledgement by the End-Customer of CE's Culture Excellence Terms and Conditions regarding CE's deliveries of services to the End-customer and/or with signature of this DPA.

Role (controller/processor): controller and (sub)processor (see below).

Data protection roles

Controller to Processor:

With respect to Processing on behalf of the End-customer and when their employees register as a user or responded to a culture assessment survey with the End-customer ("Culture Excellence Program"), the Parties acknowledge that the End-customer is the data controller and CE data processor for the Personal Data entered into the Culture Excellence Program.

The End-customer decides:

- Who has access to the Culture Excellence Program Platform data in each site (and / or a group of sites).
- How long the individuals have access to the data and if the access needs to be revoked / changed.
- Whether each individual should see all of the data or a sub-set of the data (e.g. qualitative comments are shown or hidden based on customer request).

The End-customer also provides:

- The relevant Personal Data within their company to CE.
- Requests to remove / change any of the Personal Data they have provided, if required.

Controller to Controller:

CE and the End-customer also acknowledge that there are situations outside the scope of the controller to processor situation and a need to transfer data such as invoice details, contact details, etc.

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

Categories of data subjects whose Personal Data is transferred

See table below.

Categories of Personal Data transferred

See table below.

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.

N/A

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

See table below.

Nature of the Processing

See table below.

Purpose(s) of the data transfer and further Processing

See table below.

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

See table below.

CE will Process Personal Data in accordance with the following:

Table A1A:

Categories of Personal Data collected and processed by CE	Categories of Data Subjects for which Data is Processed	Purposes for which CE Processes Personal Data	Nature of Processing	Duration of Processing
Answers to CE survey demographic questions. CE Survey Respondents answer survey questions such as "*Which option best describes your role?"* However (IMPORTANT), CE advises End-customers to not use overly granular (individual or in conjunction) organisational demographic questions (and subsequently filters) to an extent that may risk impinging anonymity; the aim of this is to prevent any single response being identifiable. No immediately or directly identifiable Respondent data is asked via demographic questions (for example, name, phone number, email address, employee ID number and other unique identifiers are not asked).	End-customer employees answering the CE surveys and other responders if/as nominated by the End-customer.	CE processes survey respondent data to create End-customer-specific scoring and other reporting content based on the CE survey responses. Demographic questions and response options map to filter types and categories which enable reported data to be filtered. In case of a situation where demographics are too granular and there are less than 5 people in a sub-group (whether in a single demographic category or when demographic types and categories are combined), the CE reporting platform has an anonymity feature to prevent these responses being shown in isolation.	Collecting, handling, storing, aggregating, reporting, sharing with sub-processors for the Processing Purposes set out adjacent.	As long as necessary for the Purposes Described in this Annex unless a longer retention is required by law. CE retains data until a deadline specified by the End-customer (End-customers are given an option of a duration of 5, 10, 15 or 20 years). End-customers specify the duration during the provision of the Services; End-customers may change their specified duration subject to a 6-month notice period.
Answers to CE survey closed questions. CE Survey Respondents evaluate survey statements such as "*There is a good team spirit"* by selecting from a set of answer options such as	Employees answering the CE surveys and other responders if/as nominated by the End-customer.	CE processes survey respondent data to create End-customer-specific scoring and other reporting content based on the aggregated CE Survey Responses. CE also processes survey respondent	Collecting, handling, storing, aggregating, reporting, sharing with sub-processors for the Processing Purposes	As long as necessary for the Purposes Described in this Annex unless a longer retention is required by law.

Categories of Personal Data collected and processed by CE	Categories of Data Subjects for which Data is Processed	Purposes for which CE Processes Personal Data	Nature of Processing	Duration of Processing
'Strongly Agree / Agree / Partly Agree / Disagree / Strongly Disagree'.		data to create aggregated and anonymised scoring and other reporting content for benchmarking and marketing Purposes. Specifically: survey closed question data is integrated with other End-customer closed question data to enable the calculation of benchmarking data.	set out adjacent.	CE retains data until a deadline specified by the End-customer (End-customers are given an option of a duration of 5, 10, 15 or 20 years). End-customers specify the duration during the provision of the Services; End-customers may change their specified duration subject to a 6-month notice period. Note: Response data is anonymised and aggregated with other End-customer data to form the basis for benchmarking reports. This aggregated data, given it's anonymisation, is retained without any deadline or fixed duration.

Categories of Personal Data collected and processed by CE	Categories of Data Subjects for which Data is Processed	Purposes for which CE Processes Personal Data	Nature of Processing	Duration of Processing
Answers to CE Survey open text questions. Comments written by Survey Respondents are open and responses may include Personal Data. However (IMPORTANT), End-customers are requested to inform Survey Respondents to not write any Personal Data into the open text fields.	End-customer employees answering the CE surveys and other responders if/as nominated by the End-customer.	CE processes survey respondent data to create End-customer-specific scoring and other reporting content based on the CE survey responses.	handling, storing, aggregating, reporting, sharing with sub-processors for the Processing Purposes set out adjacent.	As long as necessary for the Purposes Described in this Annex unless a longer retention is required by law. CE retains data until a deadline specified by the End-customer (End-customers are given an option of a duration of 5, 10, 15 or 20 years). End-customers specify the duration during the provision of the Services; End-customers may change their specified duration subject to a 6-month notice period.
User credentials User credentials permit Users to access the CE Platform and include emails, names and password hashes.	End-customer-nominated users who use an account on the CE platform to view their company's (or part of their company's) culture data, subject to the	CE uses this information to create and maintain user accounts to allow users to log into the CE Platform, and to prevent or address service, security, support or technical	Collecting, handling, storing, sharing with sub-processors, accessing and reviewing End-customer	As long as necessary for the Purposes Described in this Annex unless a longer retention is required by law.

Categories of Personal Data collected and processed by CE	Categories of Data Subjects for which Data is Processed	Purposes for which CE Processes Personal Data	Nature of Processing	Duration of Processing
	scope of the respective CE survey.	issues with the CE Platform.	Personal Data for the Processing Purposes set out adjacent.	CE retains data until a deadline specified by the End-customer (End-customers are given an option of a duration of 5, 10, 15 or 20 years). End-customers specify the duration during the provision of the Services; End-customers may change their specified duration subject to a 6-month notice period. Note: End-customer representatives may also request ad-hoc deletion of specific user accounts (for example, in the event of an employee leaving the End-customer's employ).
Professional contact details	Employees of the Sales Partner and	To enable a professional/business relationships,	Collecting, handling and storing,	As long as necessary for the Purposes

Categories of Personal Data collected and processed by CE	Categories of Data Subjects for which Data is Processed	Purposes for which CE Processes Personal Data	Nature of Processing	Duration of Processing
As part of any business relation professional details will be processed as part of (for example, but not limited to) email correspondence, webinar meetings calendar invites, internal notes, etc. Thus, this may extend to name, professional contact information (email, phone number, etc.), position, etc.	Employees of the End-customer. Employees of other cooperation partners, etc.	specifically (but not limited to) the marketing, sales, co-ordination, planning, implementation, support and follow-up of CE projects.	for the Processing Purposes set out adjacent.	Described in this Annex unless a longer retention is required by law. CE retains data until a deadline specified by the End-customer (End-customers are given an option of a duration of 5, 10, 15 or 20 years). End-customers specify the duration during the provision of the Services; End-customers may change their specified duration subject to a 6-month notice period.

For transfers to (sub-) processors, the following table outlines the subject matter, nature and duration of the Processing

Table A1B:

Company name	Subject matter	Nature of processing	Duration of the processing
Alchemer LLC	Survey response data: Responses submitted by End-customer employees.	'Raw' response data is collected via the Alchemer survey tool and stored in Alchemer database(s), to be extracted to CE's	As long as necessary for the Purposes described in this Annex unless a longer retention is required by law.

		proprietary reporting platform to be processed.	Processing durations correspond to durations outlined in Table A1A, specifically in the following sections: "*Answers to CE survey demographic questions."* And: "*Answers to CE survey closed questions."* And "*Answers to CE Survey open text questions."*
Amazon Web Services Inc. (AWS)	Names and email addresses	Automated email delivery via Amazon Simple Email Service (SES) for communication with customers for specific areas of workflow (including but not limited to welcome emails for some assessment types, survey response progress updates, survey closure notifications). Applies to email sending only. Ad-hoc emails and email receipts/ongoing conversations are covered below in this table under 'Google Inc'.	As long as necessary for the Purposes described in this Annex unless a longer retention is required by law. Processing durations correspond to durations outlined in Table A1A, specifically in the following sections: "*Professional contact details*" And "*User Credentials*"
DigitalOcean LLC	User credentials, raw and processed survey response data.	The Culture Excellence reporting platform is hosted by DigitalOcean. As such all data related to the reporting and user access thereto are stored on DigitalOcean servers.	As long as necessary for the Purposes described in this Annex unless a longer retention is required by law. Processing durations correspond to durations outlined in Table A1A, specifically in the following sections: "*Answers to CE survey demographic questions."* And: "*Answers to CE survey closed questions."*

			And "*Answers to CE Survey open text questions."* *And* "User credentials"
Google Inc.	Names, email addresses and related information (including information contained in email signatures and email content).	Ad-hoc emails related to all aspects of the Services, including sales, marketing, contracting, relationship management, scope discussion, planning, implementation, support and follow-up; managed using Gmail (the only exception is for automated email sending, as specified in the '*Amazon Web Services Inc. (AWS)*' row of this table).	As long as necessary for the Purposes described in this Annex unless a longer retention is required by law. Processing durations correspond to durations outlined in Table A1A, specifically in the following sections: "*Professional contact details*" And "*User Credentials*"
Linode LLC	User credentials, raw and processed survey response data.	Linode is used for backups of the content hosted at DigitalOcean (refer to the 'DigitalOcean' row of this table)	As long as necessary for the Purposes described in this Annex unless a longer retention is required by law. Processing durations correspond to durations outlined in Table A1A, specifically in the following sections: "*Answers to CE survey demographic questions."* And: "*Answers to CE survey closed questions."* And "*Answers to CE Survey open text questions."* *And* "User credentials"
Simply Book Me	Names and email addresses.	Simply Book Me is a scheduling tool used to reserve meeting times	As long as necessary for the Purposes described in this Annex unless a longer retention is required by law.

		between CE and End-customers.	Processing duration corresponds to the duration outlined in Table A1A, specifically in the following section: "*Professional contact details*"
Trello (Atlassian)	Names and email addresses.	Trello is used as a project management/workflow management tool by the CE team. The contact details for the End-customer project contacts (overall and per site) are tracked in Trello.	As long as necessary for the Purposes described in this Annex unless a longer retention is required by law. Processing duration corresponds to the duration outlined in Table A1A, specifically in the following section: "*Professional contact details*"

Reference is made to ANNEX III – LIST OF SUB-PROCESSORS below.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

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

The supervisory authority/ies in the Member State where the End-customer is established.

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

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

CE will store and Process the Personal Data in a manner consistent with industry security standards. CE has implemented technical, organizational and administrative systems, policies, and procedures to help ensure the security, integrity and confidentiality of Personal Data and to mitigate the risk of unauthorized access to or use of Personal Data, including:

(i) appropriate administrative, technical and physical safeguards and other security measures designed to ensure the security and confidentiality of the Personal Data it manages;

(ii) a security design intended to prevent any compromise of its own information systems, computer networks or data files by unauthorized Users, viruses or malicious computer programs; and

(iii) permitting only authorized Users access to systems and applications, and all persons with authorized access to Personal Data must have a genuine business need-to-know prior to access (together, "Security Program").

The above points are elaborated further below.

Categories of data:

Data collected, processed and stored by CE is broadly split into two areas:

- **Survey response data:** End-customer employee responses to culture assessment surveys
- **User contact data:** End-customer employee credentials (typically limited to name and email address) required to enable:
  - communications between CE and End-customer representatives before, during and afer the culture assessment (typically limited to email communication),
  - user access to the CE reporting platform to enable review of assessment results.,

CE's Security Progam applies to all data, but specific aspects are shown below that apply differently to each of these categories.

Training and Supervision:

CE maintains adequate training programs to ensure that its employees and any others acting on its behalf are aware of and adhere to its Security Program. CE shall exercise necessary and appropriate supervision over its relevant employees and any others acting in its behalf to maintain appropriate confidentiality and security of the Personal Data it manages.

Communications:

Primary communications with End-customer representatives take place on email. Such communications take place before, during and after the culture assessment to (typically) finalise scope, arrange webinars, plan and implement survey logistics, send/receive assessment progress updates, conduct ongoing Q&A and perform administrative tasks such as invoicing and contracting, CE team members use named and password protected email accounts, in addition to two generic email accounts (enquiries@culturexcellence.com and admin@culturexcellence.com) which are monitored by named members of the CE team and one generic email account (noreply@culturexcellence.com) which is not monitored. End-customer names and emails are not used for unsolicited marketing purposes, nor are they shared with any third party (with the exception of CE's sales partners) for any other marketing purpose.

End-customer site contact administration:

To enable the provision of survey progress updates to End-customer representatives (and/or where applicable to Sales P, CE collects names and email addresses for End-customer employees. Typically this includes one representative per End-customer location, and is generally a senior employee such as a quality/safety manager. This information is provided by the End-customer via Excel spreadsheets exchanged over email with the CE team (via named CE email accounts – see 'Communications' above).

Site contact spreadsheets are saved locally on CE employee laptops (temporarily) and are subsequently saved on Trello (a workflow management platform hosted by CE sub-pocessor Atlassian – for details please refer to the section on CE's sub-processors). Primary End-customer contact(s) email addresses and names are also copied into Trello fo reference by CE administrators. Access to Trello is restricted to named CE users, via password protected accounts.

Site contact names and emails are subsequently entered by named CE administrators into the CE reporting platform to enable:

- The provision of manually and automatically (system) triggered progress update emails, and/or,
- End-customer user access to assessment results on the CE platform.

Survey demographic question design:

The data collected in relation to the culture assessment suvey is designed to obfuscate the identity of the respondents. A 100% guarantee of anonymity is not possible to claim, but the identification of the physical person behind responses is made extremelty difficult, and for practical purposes, anonymity is safeguarded.

Questions at the start of the culture assessment (demographic questions) are designed to identify the demographic group of the respondent (for example, at which site does a respondent work? What is the respondent's broad category of role?). Demographic questions link to filter functionality on the reporting platform, allowing users to view data filtered by demographics (used one-by-one or in combination). For premium assessments, demographics can be customised per End-customer request. The CE team works with the End-customer representative(s) to flag and prevent the inclusion of (overly granular) demographics that would potentially result in the identification of individual employees (specifically the prevention of identifying demographic groups of less than 5 employees), whether used in isolation or in combination.

Specifically, if the CE team identifies that a combination of demographics is likely to result in less than 5 employee responses, the design is reviewed and CE recommends to the customer to remove or combine demographic questions and / or demographic question answer options. Customers may choose to over-ride CE's recommendation, but typically accept CE's (re)design advice. If the End-customer ignores or over-rides CE's recommendations the client is instructed to inform their colleagues that the data may not be anonymous prior to taking the survey.

Other (automated) assessment types do not include demgraphic customisation or design oversight by the CE team (specifically the BRCGS Food Safety Culture Excellece (FSCE) Additional Voluntary Module, the BRCGS Basic assessment and the SSAFE assessment); given design oversight is not conducted, demographic filtering is not provided in the assocated reporting. This removes the possibility of identifying individuals in the CE reporting platform front-end by their demographic grouping.

Survey respondent IP address tracking:

Internet Protocol (IP) addresses are not collected for survey resonses (removal of IP tracking also implicitely removes / disables geo-location tracking).

Directly identifiable survey response personal data:

There are no survey questions in the assessment that request directly identifiable information such as name, any form of ID (e.g. employee ID number, passport number), phone number, email address, age etc. If an End-customer requests for any such data to be collected, CE shall not comply.

Sensitive survey response personal data:

There are no survey questions in the assessment that request sensitive personal data such as gender, sexual preference(s), political affiliation, etc. If an End-customer requests for any such data to be collected, CE shall not comply.

Free text field survey response data:

Some questions allow the entry of free text by survey respndents. These questions are reported unedited to users of the platform. CE informs End-customers that they should clearly communicate to employees, prior to their response to the survey, that no personally identifiable information or data should be entered by employees into these free text questions. Finally, access to the resulting reimporting data for these questions can be switched off for an End-customer upon their request.

Raw survey response data:

Survey data is collected initially in a third party survey tool, hosted by a CE sub-processor (Alchemer.com). Response data is stored in Alchemer in raw format; data is not aggregated on the Alchemer platform, and no score calculation process takes place on the Alchemer platform. This raw response data is not made available to End-customer users in Alchemer. The data in Alchemer is only available / accessible to named CE representatives (via named password-protected accounts), in addition to Alchemer representatives. Details are available in the sub-processor section. The Alchemer servers used by CE are hosted and backed up in the EU.

Raw survey response data is extracted from Alchemer via an Application Programming Interface (API) to CE's platform servers (hosted by CE sub-processor Digital Ocean - Digital Ocean GDPR and privacy compliance information is available in the sub-processor section of CE's privacy policy). All API transfers are encrypted in flight. API access is secured by a login API token and API token secret (both unique to CE); these credentials are encrypted at rest. Access to the credentials is available to two named members of the CE team. Employees of Digital Ocean also have access. CE's platform servers (application, database and backup serviers) are hosted and backed up in the EU and UK.

Raw survey response data is accessible to two named CE resources in the backend of the CE platform. Access is password protected, Raw data (i.e. unprocessed/unaggregated response data) is available only in the back-end of the CE application, i.e. it is not accessible to CE front-end administrator users or End-customer users. Backend access passwords are managed with industry standard secure password management software. Access to the backend server(s) user interface is via username and password plus 2-factor authentication. Remote access to the backend server(s) is via SSH; there is one member of the CE team with the SSH access key, which is encryped at rest.

Access to front-end reporting:

Access is granted to users (CE users and End-Customer users) via password-protected named user accounts, Passwords are hashed using an industry standard hashing algorythm. End-customer users set their own passwords. CE provides an indicator of password strength on the password (re)set screen, but does not dictate password format, aside from enforcing a minimum of 10 characters. Password (re)set processing is only available via the user-specific registered email. Login session tokens are valid for 72 hours (tokens contain no personal data).

Front-end log-in logging:

Application event logging captures the IP address of user logins, linked to user ID (not user email or other presonal data). Logging is managed using Logstash and Elasticsearch; access is available to two named CE team members via the same credentials as the Digital Ocean backend.

Data reporting visibility – default settings:

Users access reporting data via the front-end user interface (UI) of the CE reporting platform. Some reports show the relative scoring of demographic groups. The platform will not show the data in isolation on these reports if a demographic group includes resonses from less than 5 respondents.

For example, the 'Demographic comparison' report shows scores for the demographic groups in-scope for an End-customer survey, such as roles; it presents a score summary for each role type. In this case, If there were less than 5 responses for the 'Manager' role type, the data willl not be displayed.

Data reporting visibility – filter settings:

Data can be filtered using demographic filters. Demographic filters link to the demographic questions configured in the survey itself. Further to the protection provided by the default settings outlined above, additional controls limit visibility of reporting when filters are applied.

For example, in a scenario where an End-customer has assessed 2 sites and 4 role types, the following technical rule would apply: if site 1 has 2 managers and site 2 has 3 managers, without filters applied all data would be displayed. If the End-customer user uses the filters to select the manager role type and 1 of the 2 sites, no data would be displayed and an error message would be shown to the user to indicate that there is insufficient response data to protect anonymity.

Additionally, for certain report types, not all filter options are available, due to the possibility that an End-customer could 'reverse-calculate' the contribution of an overly small demographic group. For example, the 'Response Distribution' report shows how responses spread across the various answer options; for this report, the role demographic filter is removed and cannot be used.

Note: additional information is available in the CE Pivacy Policy documentation – available upon request (please email admin@culturexcellence to request this).

Additional obfuscation of respondent identity:

When End-customer employees respond to survey demographic questions, specifically when they answer the role question, they are presented with multiple options; typically the following:

- Manager / Senior Manager
- Supervisor / Team Leader
- Operator / Operative
- Temporary Operator

Neither CE nor the End-customer enforces which answer a particular employee selects. It has been the case, and could, at any time for any End-customer, be the case, that an employee of any hierarchy level could, deliberately or by accident, select the wrong role. After that employee submits their response, there is no way to know whether or not they have submitted the appropriate / accurate role selection. This is primarily because no unique individual empoloyee-specific data is collected (as described earlier in this document).

Therefore, even in the case of (for example) an End-customer site with only 1 Manager, which may result in just one record in the database with the 'Manager' role type, it is not possible to conclude with 100% certainty that the response was, in fact, submitted by the manager at the site (for example, the manager may have accidentally selected 'Supervisor' and another empoyee may have accidentally selected 'Manager'). This means that such a response cannot be definitively identified as the site manager's response. As such, this lends further obfuscation of individual employee responses.

Cookies:

CE maintains dedicated documentation related to use of Cookies – this is available upon request (please email admin@culturexcellence.com to request this).

ANNEX III – LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of processorsub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

Company name	**Registered office**	**Contact details**	**Data storage location**	**Data protection mechanisms**
Alchemer LLC	USA	compliance@alchemer.com	EU	Privacy policy GDPR policy
Amazon Web Services Inc.	USA	Attention: General Counsel 410 Terry Avenue North Seattle, WA.	EU	Privacy policy
DigitalOcean LLC	USA	privacy@digitalocean.com	EU	Privacy policy GDPR policy
Google Inc.	USA	https://support.google.com	EU	Privacy policy
Linode LLC	USA	privacy@linode.com	EU	Privacy policy Compliance policy
Simply Book Me	Cypress	legal@simplybook.me	EU	Privacy policy
Trello (Atlassian)	USA	privacy@atlassian.com	EU	Privacy policy

ANNEX IV – STANDARD DATA PROTECTION CLAUSES TO BE ISSUED BY THE COMMISSIONER UNDER S119A(1) UK DATA PROTECTION ACT 2018

International Data Transfer Addendum to the EU Commission Standard Contractual Clauses

VERSION B1.0, in force 21 March 2022

This Addendum has been issued by the Information Commissioner for Parties making Restricted Transfers. The Information Commissioner considers that it provides Appropriate Safeguards for Restricted Transfers when it is entered into as a legally binding contract.

Part 1: Tables

Table 1: Parties

Start date	Enters into force along with the Parties' signing of an applicable commercial agreement.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	Full legal name: The End-customer: Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture Excellence Terms and Conditions and/or the details provided on the signature page of this DPA. Main address (if a company registered address): Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture Excellence Terms and Conditions and/or the details provided on the signature page of this DPA. Official registration number (if any) (company number or similar identifier): Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture	Full legal name: Culture Excellence Main address (if a company registered address): DSO-DDP-A5-D-FLEX-G001, Building A5, Dubai Silicon Oasis, Dubai, United Arab Emirates Official registration number (if any) (company number or similar identifier): 37354

	Excellence Terms and Conditions and/or the details provided on the signature page of this DPA.	
Key Contact	Full Name (optional): Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture Excellence Terms and Conditions and/or the details provided on the signature page of this DPA. Job Title: Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture Excellence Terms and Conditions and/or the details provided on the signature page of this DPA. Contact details including email: Reference is made to the commercial agreement between the Parties and/or the details provided by the End-customer, when the End-Customer acknowledged the CE Culture Excellence Terms and Conditions and/or the details provided on the signature page of this DPA.	Full Name (optional): David Shannon Job Title: Owner and Technical Director Contact details including email: dave@culturexcellence.com
Signature (if required for the Purposes of Section 2)	Reference is made to the commercial agreement between the Parties and/or to the End-Customer's acknowledgement of the CE Culture Excellence Terms and Conditions regarding CE's deliveries of services to the End-customer and/or to the signature page of this DPA.	Reference is made to the commercial agreement between the Parties and/or to the End-Customer's acknowledgement of the CE Culture Excellence Terms and Conditions regarding CE's deliveries of services to the End-customer and/or to the signature page of this DPA.

Table 2: Selected SCCs, Modules and Selected Clauses

Addendum EU SCCs	The version of the Approved EU SCCs which this Addendum is appended to, detailed below, including the Appendix Information: Reference is made to the above.

Module	Module in operation	Clause 7 (Docking Clause)	Clause 11 (Option)	Clause 9a (Prior Authorisation or General Authorisation)	Clause 9a (Time period)	Is Personal Data received from the Importer combined with Personal Data collected by the Exporter?
1						
2						
3						
4						

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: Reference is made to Appendix 1 above.
Annex 1B: Description of Transfer: Reference is made to Appendix 1 above.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: Reference is made to ANNEX II - TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA above.
Annex III: List of sub-processors (Modules 2 and 3 only): Reference is made to ANNEX III – LIST OF SUB-PROCESSORS

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 19: X Importer X Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

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

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

Interpretation of this Addendum

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

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.
Appropriate Safeguards	The standard of protection over the Personal Data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 18.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.

UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the Processing of Personal Data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

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

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

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

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

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

Hierarchy

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

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

11. Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

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

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

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

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

and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

13. Unless the Parties have agreed alternative amendments which meet the requirements of Section 12, the provisions of Section 15 will apply.

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

15. The following amendments to the Addendum EU SCCs (for the Purpose of Section 12) are made:

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

    b. In Clause 2, delete the words:

        "and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679";

    c. Clause 6 (Description of the transfer(s)) is replaced with:

        "The details of the transfers(s) and in particular the categories of Personal Data that are transferred and the Purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's Processing when making that transfer.";

    d. Clause 8.7(i) of Module 1 is replaced with:

        "it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

    e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

        "the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

    f. References to "Regulation (EU) 2016/679", "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data (General Data Protection Regulation)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

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

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

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

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

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

    l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of Personal Data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

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

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

Amendments to this Addendum

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

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

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

    a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
    b. reflects changes to UK Data Protection Laws;

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

19. If the ICO issues a revised Approved Addendum under Section 18, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

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

    b its risk under the Addendum,

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

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

Alternative Part 2 Mandatory Clauses:

Mandatory Clauses	Part 2: 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.

ANNEX V – DEFINITIONS

1. **Definitions: T**he terms set out below shall be defined as follows:

a) "**Culture Excellence Program**" is defined as the provision of an assessment of culture and reporting of results, across a range of specific assessment types, scopes, reporting formats and support options and as further outlined at https://culturexcellence.com.

b) "**Data Subjects**" means all physical persons whose Personal Data is processed under this agreement, hereunder Users, Survey Respondents, contact persons of the End-customer, etc.

c) "**End-customer"** means the company or other organisation purchasing the culture assessment survey / Culture Excellence Program. The End-customer is the data controller for the Personal Data entered into the Culture Excellence Program.

d) "**Personal Data**" means any information relating to an identified or identifiable natural person which (i) End-customer provides to CE, or (ii) CE obtains from other parties, in each case in connection with the agreement and/or the Purposes.

e) "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, the Personal Data transmitted, stored or otherwise Processed.

f) "**Processing**" (including "**Process**" and "**Processed**") means any operation(s) performed on Personal Data, whether or not by automated means, including the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

g) "**Purposes**" means (i) the provision, administration and promotion of the Services and upgrades to the Services, (ii) communicating with site contacts, including responding to their enquiries; and (iii) sending out surveys to site contacts, monitoring the results of those surveys, and provision of support during and post-survey.

h) "**Services**" is defined as the assessment and reporting of organisational culture with a specific focus on sub-types of culture including food safety, product safety, quality, health and safety, environmental sustainability and general engagement. The assessment involves a collection of survey responses from a representative sample of End-customer employees, followed by the processing of the response data and the generation of reporting to highlight areas of strength, weakness and risk. Assessments are supported by instructional documents, webinars meetings, and supplemented by post-assessment webinars and action planning. There are various types of assessment, which differ in terms of scope, amount of data reported and amount of support provided. At the time of writing, the types of assessment provided are the following:

a. Premium assessment: full scope, customisable, with all support options available, 1000+ data points.

b. BRCGS assessment: food safety scope, no customisation, PDF instructions, pre-recorded general webinars, ~65 data points.

c. BRCGS Basic: free-of-charge sample assessment, food safety scope, no customisation, PDF instructions, pre-recorded general webinars, subset of survey questions, ~9 data points. Not representative of culture – limited to 6 responses – intended as a sample of the assessment process only.

d. SSAFE: free-of-charge sample assessment, food safety scope, no customisation, PDF instructions, pre-recorded general webinars, subset of survey questions, ~10 data points.

i) "**Survey Respondent(s)**" means data subjects that have answered CE surveys.

j) "Terms and Conditions" means, but is not limited to, the terms and conditions maintained on the following webpages:

a. https://www.culturexcellence.com/general-terms, and

b. https://www.culturexcellence.com/privacy, and

c. https://www.culturexcellence.com/cookies.

k) "**CE Platform**" means the online data platform created by CE and accessed by Partner(s) and / or User(s), currently hosted at https://platform.culturexcellence.com and https://app.culturexcellence.com.

l) "**User**" means, as the case may be, any employee of an End-customer who is provided access to the CE Platform, as well as CE employees who administer the CE Platform.

SIGNATURE PAGE

For and on behalf of the End-customer:
Name:

Role/Position/Job title:

Contact email:

Company legal name:

Registered company address:

Company registration number:

Signature:

Date:

For and on behalf of Culture Excellence:
Name: David Shannon
Role/Position/Job title: Technical Director
Contact email: dave@culturexcellence.com
Company legal name: Culture Excellence
Registered company address: DSO-DDP-A5-D-FLEX-G001, Building, A5, Dubai Silicon Oasis, Dubai, UAE
Company registration number: 37354
Signature:

Date: 11th April 2024