Data Protection Addendum

This Data Protection Addendum ("**Addendum**") forms part of the _____ ("**Principal Agreement**") between: (i) _____ **("Vendor")** acting on its own behalf and as agent for each Vendor Affiliate;[1] and (ii) **Organosi** ("**Company**") acting on its own behalf and as agent for each Company Affiliate.

The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 "**Applicable Laws**" means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Company Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Company Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Company, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise;[2]

1.1.3 "**Company Group Member**" means Company or any Company Affiliate;

---

1 Parties to consider whether to adopt a group-to-group contracting structure, as here, and the practicalities of ensuring that each party is properly authorised to enter into the Addendum on behalf of its Affiliates.

2 The Controller will need to examine this definition and consider whether it is broad enough given its group structure.

1.1.4 "**Company Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of a Company Group Member[3] pursuant to or in connection with the Principal Agreement;

1.1.5 "**Contracted Processor**" means Vendor or a Subprocessor;

1.1.6 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;[4]

1.1.7 "**EEA**" means the European Economic Area;

1.1.8 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR[5];

1.1.9 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.10 "**Restricted Transfer**" means:

1.1.10.1 a transfer of Company Personal Data from any Company Group Member to a Contracted Processor; or

1.1.10.2 an onward transfer of Company Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under section [6.4.3 or][6] 12 below;[7]

---

3 Controller to consider expanding if Processor may process personal data on behalf of unaffiliated third parties (such as customers) as well as Affiliates. If a wider definition is required, then consequential amendments will likely be required to the substantive provisions in this Addendum, for example in relation to Restricted Transfers.

4 This drafting is intended to include laws replacing the GDPR in the UK after Brexit.

5 Given the terms of reference of the IRSG working group which developed this template Addendum, which were limited to Article 28 GDPR, transfer and related issues, this proposed definition is quite narrowly drawn only referring to the core Directive 95/46/EC and to GDPR. The parties will need to consider whether a wider definition, including reference to the E-Privacy Directive (and its proposed replacement) and potentially to interception and other data related laws is more appropriate for its purposes.

6 See footnotes 14 and 27 below.

7 The parties might consider "avoidance of doubt" wording here, to more clearly identify transfers which would and would not be Restricted Transfers – for example:

"For the avoidance of doubt: (a) without limitation to the generality of the foregoing, the parties to this Addendum intend that transfers of Personal Data from the UK to the EEA or from the EEA to the UK, following any exit by the UK from the European Union shall be Restricted Transfers for such time and to such extent that such transfers would be prohibited by Data Protection Laws of the UK or EU Data Protection Laws (as the case may be) in the absence of the Standard Contractual Clauses to be

1.1.11 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of Vendor for Company Group Members pursuant to the Principal Agreement;

1.1.12 "**Standard Contractual Clauses**" means the contractual clauses set out in Annex 2, amended as indicated (in square brackets and italics) in that Annex and under section 13.4;

1.1.13 "**Subprocessor**" means any person (including any third party and any Vendor Affiliate, but excluding an employee of Vendor or any of its sub-contractors) appointed by or on behalf of Vendor or any Vendor Affiliate to Process Personal Data on behalf of any Company Group Member in connection with the Principal Agreement; and

1.1.14 "**Vendor Affiliate**" means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with Vendor, where control is defined as the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of an entity, whether through ownership of voting securities, by contract or otherwise.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**",[8] "**Personal Data Breach**", "**Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Authority

Vendor warrants and represents that, before any Vendor Affiliate Processes any Company Personal Data on behalf of any Company Group Member, Vendor's entry into this Addendum as agent for and on behalf of that Vendor Affiliate will have been duly and effectively authorised (or subsequently ratified) by that Vendor Affiliate.[9]

established under section [6.4.3 or] 12; and (b) where a transfer of Personal Data is of a type authorised by Data Protection Laws in the exporting country, for example in the case of transfers from within the European Union to a country (such as Switzerland) or scheme (such as the US Privacy Shield) which is approved by the Commission as ensuring an adequate level of protection or any transfer which falls within a permitted derogation, such transfer shall not be a Restricted Transfer;"

8 The GDPR definition of "personal data" will not include personal data relating to legal persons other than individuals, so if a firm wishes to extend the scope of the Addendum to cover processing under the laws of e.g. Switzerland or South Africa a wider definition should be considered here. (Note that this change is already made in the Standard Contractual Clauses in Annex 2.)

9 This is not essential for the purposes of GDPR compliance (although see footnotes 14 and 27 below regarding the use of the Standard Contractual Clauses).

3. Processing of Company Personal Data

3.1 Vendor and each Vendor Affiliate shall:

3.1.1 comply with all applicable Data Protection Laws in the Processing of Company Personal Data;[10] and

3.1.2 not Process Company Personal Data other than on the relevant Company Group Member's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case Vendor or the relevant Vendor Affiliate shall to the extent permitted by Applicable Laws inform the relevant Company Group Member of that legal requirement before the relevant Processing of that Personal Data.

3.2 Each Company Group Member:

3.2.1 instructs Vendor and each Vendor Affiliate (and authorises Vendor and each Vendor Affiliate to instruct each Subprocessor) to:

3.2.1.1 Process Company Personal Data; and

3.2.1.2 in particular, transfer Company Personal Data to any country or territory, as reasonably necessary for the provision of the Services and consistent with the Principal Agreement; and

3.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 3.2.1 on behalf of each relevant Company Affiliate[11].

3.3 Annex 1 to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Company Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). Company may make reasonable amendments to Annex 1 by written notice to Vendor from time to time as Company reasonably considers necessary to meet those requirements. Nothing in Annex 1 (including as amended pursuant to this section 3.3) confers any right or imposes any obligation on any party to this Addendum.

4. Vendor and Vendor Affiliate Personnel

Vendor and each Vendor Affiliate shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Company Personal Data, ensuring in each case that access is strictly limited to those individuals

10 This is not essential for the purposes of GDPR compliance and, of course, may repeat a provision already included in the Principal Agreement.

11 Although not required by GDPR, vendors will want to ensure that where a controller affiliate is issuing instructions on behalf of other affiliates in its group that it has authority to do so.

who need to know / access the relevant Company Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

5. Security[12]

5.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Vendor and each Vendor Affiliate shall in relation to the Company Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

5.2 In assessing the appropriate level of security, Vendor and each Vendor Affiliate shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

6. Subprocessing

Neither Vendor nor any Vendor Affiliate shall appoint (nor disclose any Company Personal Data to) the proposed Subprocessor except with the prior written consent of Company.

6.1 With respect to each Subprocessor, Vendor or the relevant Vendor Affiliate shall:

6.1.1 before the Subprocessor first Processes Company Personal Data (or, where relevant, in accordance with section 6.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Company Personal Data required by the Principal Agreement;

6.1.2 ensure that the arrangement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms

---

12 As the GDPR imposes on Vendor a requirement to ensure that appropriate security measures are in place, and Vendor may not be in a position to assess what measures are appropriate to the Company Personal Data (since the data are collected and processed for the purposes of Company's and not Vendor's business), Vendor may seek protection against contracted security measures turning out not to be appropriate although they have been approved (and may even have been specifically selected) by Company. It may also be the case that specific security measures are identified in the Principal Agreement. The GDPR does not (or at least does not clearly) change the actual standard of security required. The Company as Controller may wish to elaborate on the approach taken here, for example by:

- committing Vendor only to a specific, relatively basic, level of security, described (in generic terms) in an Annex, with Company taking responsibility for any higher level of security required by the GDPR except to the extent specifically agreed (including in the Principal Agreement); or
- confirming that Company has assessed any security measures specifically agreed in the Principal Agreement and that the Company is responsible (as between the parties and to data subjects and supervisory authorities) if those measures, in themselves (but acknowledging that any pre-agreed description may only deal with specific aspects of the required security arrangements rather than describing a comprehensive solution), do not meet the GDPR standard of appropriateness.

which offer at least the same level of protection for Company Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;[13]

6.1.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) Vendor, or (b) the relevant Vendor Affiliate, or (c) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Company Personal Data procure that it enters into an agreement incorporating the Standard Contractual Clauses with the relevant Company Group Member(s) (and Company shall procure that each Company Affiliate party to any such Standard Contractual Clauses co-operates with their population and execution);[14] and

6.1.4 provide to Company for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as Company may request from time to time.

6.2 Vendor and each Vendor Affiliate shall ensure that each Subprocessor performs the obligations under sections 3.1, 4, 5, 7.1, 8.2, 9 and 11.1, as they apply to Processing of Company Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of Vendor.

7. Data Subject Rights[15]

7.1 Taking into account the nature of the Processing, Vendor and each Vendor Affiliate shall assist each Company Group Member by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company Group Members'

13 Article 28(4) requires a processor to appoint any subprocessor on "the same" terms on which it is appointed by the controller. There is therefore a risk that this language will amount to a technical breach of article 28(4), since it allows Vendor (as processor) to use different terms as long as they are at least as protective and meet the requirements of article 28(3). It is of course open to Vendor to meet its obligations under article 28(4) more literally, irrespective of this provision, and arguably article 28(4) does not bind Company as the Controller.

14 This approach – with the default position being to require the Vendor to enter into a contract incorporating the Standard Contractual Clauses with the Subprocessor – is not really necessary if Vendor is itself outside the EEA (because the necessary requirement is imposed on Vendor through clause 11 of the Standard Contractual Clauses); and it is not technically sufficient if Vendor is within the EEA, since in those circumstances the Standard Contractual Clauses should in principle be put in place directly between the relevant Company Group Member(s) and the non-EEA Subprocessor. The approach is, nonetheless, not uncommon. See section 12.4 and footnote 27 for an alternative approach. Alternatively, Vendor could be required to ensure that direct standalone agreements incorporating the Standard Contractual Clauses are put in place with each Subprocessor that is party to a Restricted Transfer, but of course this may be problematic logistically.

15 Sections 7 and 9 could in principle be combined into a simpler (although more sweeping, and therefore more onerous from Vendor's perspective) co-operation provision. Regarding both of these sections and section 8, the parties will need to consider the commercial implications of Vendor co-operation (in particular, whether, in what circumstances and on what basis Vendor might be entitled to recover its costs incurred in assisting Company).

obligations, as reasonably understood by Company, to respond to requests to exercise Data Subject rights under the Data Protection Laws[16].

7.2 Vendor shall:

7.2.1 promptly notify Company if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data; and

7.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of Company or the relevant Company Affiliate or as required by Applicable Laws to which the Contracted Processor is subject, in which case Vendor shall to the extent permitted by Applicable Laws inform Company of that legal requirement before the Contracted Processor responds to the request.

8. Personal Data Breach

8.1 Vendor shall notify Company without undue delay upon Vendor or any Subprocessor becoming aware of a Personal Data Breach affecting Company Personal Data, providing Company with sufficient information to allow each Company Group Member to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.[17]

8.2 Vendor shall co-operate with Company and each Company Group Member and take such reasonable commercial steps as are directed by Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

9. Data Protection Impact Assessment and Prior Consultation

Vendor and each Vendor Affiliate shall provide reasonable assistance to each Company Group Member with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Company reasonably considers to be required of any Company Group Member by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation

16 Given the potentially wide scope of this obligation another approach which is likely to be more palatable for vendors would be to specify any specific technical measures that will be implemented by the processor, together with an acknowledgment by the controller and the processor that they consider these measures to be appropriate, taking into account the nature of the processing.

17 Controllers may wish to be more specific as to the information to be provided, e.g.: "*Such notification shall as a minimum:*

8.1.1 describe the nature of the Personal Data Breach, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

8.1.2 communicate the name and contact details of Vendor's data protection officer or other relevant contact from whom more information may be obtained;

8.1.3 describe the likely consequences of the Personal Data Breach; and

8.1.4 describe the measures taken or proposed to be taken to address the Personal Data Breach."

to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

10. Deletion or return of Company Personal Data[18]

10.1 Subject to sections 10.2 and 10.3 Vendor and each Vendor Affiliate shall promptly and in any event within [ ][19] of the date of cessation of any Services involving the Processing of Company Personal Data (the "**Cessation Date**"), delete[20] and procure the deletion of all copies of those Company Personal Data.

10.2 Subject to section 10.3, Company may in its absolute discretion by written notice to Vendor within [ ][21] of the Cessation Date require Vendor and each Vendor Affiliate to (a) return a complete copy of all Company Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Vendor; and (b) delete and procure the deletion of all other copies of Company Personal Data Processed by any Contracted Processor. Vendor and each Vendor Affiliate shall comply with any such written request within [ ][22] of the Cessation Date.

10.3 Each Contracted Processor may retain Company Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that Vendor and each Vendor Affiliate shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

10.4 Vendor shall provide written certification to Company that it and each Vendor Affiliate has fully complied with this section 10 within [ ][23] of the Cessation Date.

---

18 The parties may consider alternatively providing for return of data by default, with deletion only if specified by Company at the time. If the Addendum is to be used with a large number of Vendors, default deletion may lead to unconsidered deletion of data needed by Company.

19 The parties to specify period – the GDPR does not set any particular period.

20 The parties might consider defining the word "**delete**" to make clear that it means definitive deletion, permanently removing all copies in Vendor's systems. For example:

> "***"Delete"*** *means to remove or obliterate Personal Data such that it cannot be recovered or reconstructed;*"

Article 28 does not require this clarification. If it is not made, Vendors may seek to interpret the term more "softly", which may ultimately be inconsistent with the correct interpretation of article 28 (taking into account, for example, future regulatory guidance). Having said that, use of the term without definition should be sufficient to meet the requirements of article 28(3), and including a definition may prompt comments from and therefore a need for negotiation with Vendors.

21 The parties to specify period – the GDPR does not set any particular period.

22 The parties to specify period – the GDPR does not set any particular period.

23 The parties to specify period – the GDPR does not set any particular period.

11. Audit rights

11.1 Subject to sections [11.2 to 11.4], Vendor and each Vendor Affiliate shall make available to each Company Group Member on request all information[24] necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by any Company Group Member or an auditor mandated by any Company Group Member in relation to the Processing of the Company Personal Data by the Contracted Processors.

11.2 Information and audit rights of the Company Group Members only arise under section 11.1 to the extent that the Principal Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

11.3 [A Company Group Member may only mandate an auditor for the purposes of section 11.1 if the auditor is identified in the list set out in Annex 3 to this Addendum, as that list is amended by agreement between the parties in writing from time to time. Vendor shall not unreasonably withhold or delay agreement to the addition of a new auditor to that list.]

11.4 [Company or the relevant Company Affiliate undertaking an audit shall give Vendor or the relevant Vendor Affiliate reasonable notice of any audit or inspection to be conducted under section 11.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

11.4.1 to any individual unless he or she produces reasonable evidence of identity and authority;

11.4.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and Company or the relevant Company Affiilate undertaking an audit has given notice to Vendor or the relevant Vendor Affiliate that this is the case before attendance outside those hours begins; or

---

24 This Addendum does not seek to address the text at the end of article 28(3) ("*With regard to point (h) of the first subparagraph, the processor shall immediately inform the controller if, in its opinion, an instruction infringes this Regulation or other Union or Member State data protection provisions.*") It is not yet clear whether this text requires a processor, in the context of its information obligations referred to in article 28(3)(h), to inform the controller if it considers that ***any processing instruction*** is likely to lead to a breach of EU data protection law; or whether it only requires a processor to inform the controller if it considers that ***an instruction given in relation to an audit under article 28(3)(h)*** is likely to lead to such a breach. In any case, the text at the end of article 28(3), while it clearly imposes an obligation on the processor, does not clearly require the inclusion of a provision in the contract between the controller and the processor. Very cautiously, a firm might consider seeking to address this point, e.g. (if the second possible interpretation of the text is adopted): "*Vendor shall immediately inform Company if, in its opinion, an instruction pursuant to this section 11 (Audit Rights) infringes the GDPR or other EU or Member State data protection provisions*".

11.4.3 for the purposes of more than [one] audit or inspection, in respect of each Contracted Processor, in any [calendar year], except for any additional audits or inspections which:

11.4.3.1 Company or the relevant Company Affiliate undertaking an audit reasonably considers necessary because of genuine concerns as to Vendor's or the relevant Vendor Affiliate's compliance with this Addendum; or

11.4.3.2 A Company Group Member is required or requested to carry out by Data Protection Law, a Supervisory Authority or any similar regulatory authority responsible for the enforcement of Data Protection Laws in any country or territory,

where Company or the relevant Company Affiliate undertaking an audit has identified its concerns or the relevant requirement or request in its notice to Vendor or the relevant Vendor Affiliate of the audit or inspection.]

12. Restricted Transfers

12.1 Subject to section 12.3, each Company Group Member (as "data exporter") and each Contracted Processor, as appropriate,[25] (as "data importer") hereby enter into the Standard Contractual Clauses in respect of any Restricted Transfer from that Company Group Member to that Contracted Processor.

12.2 The Standard Contractual Clauses shall come into effect under section 12.1 on the later of:

12.2.1 the data exporter becoming a party to them;

12.2.2 the data importer becoming a party to them; and

12.2.3 commencement of the relevant Restricted Transfer.

12.3 Section 12.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Law.

12.4 [Vendor warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor which is not a Vendor Affiliate[26], Vendor's or the relevant Vendor Affiliate's entry into the Standard Contractual Clauses under section 12.1, and agreement to variations to those Standard Contractual Clauses made under section 13.4.1, as agent for and on behalf

25 See footnote 27 below.

26 Vendor Affiliates are excluded because Vendor's authority on behalf of Vendor Affiliates is addressed in section 2.

of that Subprocessor will have been duly and effectively authorised (or subsequently ratified) by that Subprocessor.][27]

13. General Terms

Governing law and jurisdiction

13.1 Without prejudice to clauses 7 (Mediation and Jurisdiction) and 9 (Governing Law) of the Standard Contractual Clauses:

13.1.1 the parties to this Addendum hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

13.1.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement. [28]

Order of precedence[29]

13.2 Nothing in this Addendum reduces Vendor's or any Vendor Affiliate's obligations under the Principal Agreement in relation to the protection of Personal Data or permits Vendor or any Vendor Affiliate to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement. In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

---

27 See footnote 14 above. Section 12.4 represents an alternative, more fully effective, approach, through which a direct agreement incorporating the standard contractual clauses is put in place between the relevant Company Group Member and the non-EEA Subprocessor. However it depends on Vendor being authorised by the Subprocessor to enter into the standard contractual clauses as agent on its behalf, which may be problematic from Vendor's perspective.

28 Article 28(3) of the GDPR can be read as requiring any agreement between a controller and a processor, or any agreement binding a Subprocessor in order to meet the requirements of article 28(3), to be governed by EU or EU member state law. There is, therefore, a risk that a technical breach of article 28(3) will arise if the Principal Agreement is governed by the law of a third country or if Vendor enters into a subcontract with a Subprocessor which is governed by the law of a third country. There are, however, also arguments to the contrary (either:

- on the basis that the requirement is to put in place either a contract (which can be governed by the law of any country) or an "other legal act" (which must be governed by EU or member state law), given that, after all, it is not possible for an agreement to be governed by "EU" law; or
- on the basis that the requirement is for the agreement to be "*a legal act under*" EU or member state late – that is, something recognised by law within the EU, which would include a contract governed by the laws of a third country - rather than for it to be *governed by* EU or member state law.)

If the parties are unwilling to live with even this technical risk, they could include provisions requiring the Addendum and any contract with a Subprocessor to be governed by the law of a Member State where EU Data Protection Laws apply. The parties should also consider including equivalent provisions to deal with a situation where an equivalent to article 28(3) arising under post-Brexit UK law imposes an equivalent requirement.

29 Included to ensure that these Article 28 ready terms prevail.

13.3 Subject to section 13.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

13.4 Company may:

13.4.1 by at least [30 (thirty) calendar days'] written notice to Vendor from time to time make any variations to the Standard Contractual Clauses (including any Standard Contractual Clauses entered into under section 12.1), as they apply to Restricted Transfers which are subject to a particular Data Protection Law, which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

13.4.2 propose any other variations to this Addendum which Company reasonably considers to be necessary to address the requirements of any Data Protection Law.

13.5 If Company gives notice under section 13.4.1:

13.5.1 [Vendor and each Vendor Affiliate shall promptly co-operate (and ensure that any affected Subprocessors promptly co-operate) to ensure that equivalent variations are made to any agreement put in place under section 6.4.3; and]

13.5.2 Company shall not unreasonably withhold or delay agreement to any consequential variations to this Addendum proposed by Vendor to protect the Contracted Processors against additional risks associated with the variations made under section 13.4.1 [and/or 13.5.1].

13.6 If Company gives notice under section 13.4.2, the parties shall promptly discuss the proposed variations and negotiate in good faith with a view to agreeing and implementing those or alternative variations designed to address the requirements identified in Company's notice as soon as is reasonably practicable.

13.7 Neither Company nor Vendor shall require the consent or approval of any Company Affiliate or Vendor Affiliate to amend this Addendum pursuant to this section 13.5 or otherwise.

Severance

13.8 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties'

intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

ORGANOSI

Signature _____

Name _____

Title _____

Date Signed _____

[Vendor]

Signature _____

Name _____

Title _____

Date Signed _____

ANNEX 1: DETAILS OF PROCESSING OF COMPANY PERSONAL DATA

This Annex 1 includes certain details of the Processing of Company Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the Processing of Company Personal Data

The subject matter and duration of the Processing of the Company Personal Data are set out in the Principal Agreement and this Addendum.

The nature and purpose of the Processing of Company Personal Data

[Include description here]

The types of Company Personal Data to be Processed

[Include list of data types here]

The categories of Data Subject to whom the Company Personal Data relates

[Include categories of data subjects here]

The obligations and rights of Company and Company Affiliates

The obligations and rights of Company and Company Affiliates are set out in the Principal Agreement and this Addendum.

ANNEX 2: STANDARD CONTRACTUAL CLAUSES[30]

[*These Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Law*[31] *(otherwise).*]

[*If these Clauses are not governed by the law of a Member State, the terms "Member State" and "State" are replaced, throughout, by the word "jurisdiction".*]

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection [*This opening recital is deleted if these Clauses are not governed by the law of a member state of the EEA.*]

[*The gaps below are populated with details of the relevant Company Group Member:*]

Name of the data exporting organisation:

Address:

Tel.: _____; fax: _____; e-mail: _____

Other information needed to identify the organisation

.....

(the data **exporter**)

And

[*The gaps below are populated with details of the relevant Contracted Processor:*]

Name of the data importing organisation:

---

30 The Standard Contractual Clauses could be included by cross-reference, rather than being set out in full, for brevity. However: (i) this would require statement (in an Annex or in the body of the Addendum) of the *population* of the Standard Contractual Clauses; and (ii) since their content is likely either to be very well known to a given Vendor or to be irrelevant because no Restricted Transfers will be made, their inclusion is unlikely in itself to concern Vendors.

31 The standard clauses are of course approved by the European Commission and not by any equivalent authority. The reference here is intended to capture possible deemed approval of the same standard clauses by an equivalent UK authority on or after Brexit (or, in theory, an equivalent authority in another departing Member State in the future).

Address:

Tel.: _____; fax: _____; e-mail:_____

Other information needed to identify the organisation:

.....

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Background

The data exporter has entered into a data processing addendum ("DPA") with the data importer. Pursuant to the terms of the DPA, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. Data importer is located in a country not ensuring an adequate level of data protection. To ensure compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such Services, including the processing of personal data incidental thereto, subject to the data importer's execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [*If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words "except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data" are added.*]

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC" are deleted.*]

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only

on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC; [*If these Clauses are not governed by the law of a Member State, the words "within the meaning of Directive 95/46/EC" are deleted.*]

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or

have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

   (b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:
[*Populated with details of, and deemed signed on behalf of, the data exporter:*]
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature.....

On behalf of the data importer:
[*Populated with details of, and deemed signed on behalf of, the data importer:*]
Name (written out in full):
Position:
Address:
Other information necessary in order for the contract to be binding (if any):

Signature.....

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties
The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter
The data exporter is:
[TO BE COMPLETED]

Data importer
The data importer is:
[TO BE COMPLETED]

Data subjects
The personal data transferred concern the following categories of data subjects:
[TO BE COMPLETED]

Categories of data
The personal data transferred concern the following categories of data:
[TO BE COMPLETED]

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data:
[TO BE COMPLETED]

Processing operations
The personal data transferred will be subject to the following basic processing activities:

[TO BE COMPLETED]

DATA EXPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data exporter:*]
Name:……
Authorised Signature ……
DATA IMPORTER

[*Populated with details of, and deemed to be signed on behalf of, the data importer:*]
Name:……
Authorised Signature ……

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

[TO BE COMPLETED]

ANNEX 3: LIST OF MANDATED AUDITORS

[TO BE COMPLETED]