Comprehensive Data Processing Addendum
(ICF Next SA_Vendor Facing)

This Data Protection Addendum ("**DPA**") applies to the Vendor's Processing of Personal Data for the provision of the Services specified in the Suppliers Agreement, SOW or Purchase Order ("**Agreement**"). Both Vendor and ICF may also be referred to as "Party" or may collectively be referred to as the "Parties".

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 Agreement. Except where the context requires otherwise, references in this Addendum to the Agreement are to the Agreement as amended by, and including, this Addendum.

1. Definitions

1.1. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified in Appendix A, the terms of the Agreement shall remain in full force and effect. This DPA contains ICF's Technical and Operational Measures and Procedures which are in addition to and cumulative of the requirements of the Agreement.

2. Roles of the Parties

2.1 As agreed between the Parties for the Processing of Personal Data, ICF shall be the Data Controller and the Vendor shall be the Data Processor. However, where ICF is engaging the Vendor for the provision of Services for and on behalf of a client of ICF ("**ICF Client**"):

2.1.1 Vendor shall abide by data protection terms from ICF's Client as incorporated into the Agreement or in the applicable Statements of Work or related orders forms ("**SOWs**"). The data controller will be the relevant ICF Client as identified in relevant SOWs, the data processor will be ICF as the contractor of the ICF Client, and the Vendor is the data (sub)processor under Article 29 of the GDPR, or when applicable, under Article 29(4) of the Regulation (EU) 2018/1725.

2.1.2 ICF will serve as a point of contact for Vendor and will provide all notifications and or seeking appropriate authorisations from the relevant ICF Client (Data Controller).

2.2 The Parties agree that each Party shall be solely responsible for determining their respective obligations stemming from Data Protection Laws and Regulations and for ensuring compliance with such obligations. In no event will either Party be required to monitor or advise the other regarding the Data Protection Laws and Regulations, including obligations stemming from these, applicable to the other Party with respect to Personal Data.

3. Processing of Personal Data

3.1 At all times during the term of this DPA the Vendor shall (and will ensure that its employees):

3.1.1 process the types of Personal Data relating to the categories of Data Subjects for the specific purposes in each case as set forth in Annex 1 to this DPA ("**Details of the Processing**").

3.1.2 process Personal Data on ICF's behalf and in accordance with ICF's documented instructions for the following purposes: (i) Processing in accordance with the Agreement and applicable SOWs; (ii) Processing initiated by ICF in their use of the Services; and (iii) Processing to comply with other documented reasonable instructions provided by ICF (e.g., via email) where such instructions are consistent with the terms of the Agreement. If Vendor reasonably believes that an instruction given by ICF violates any Data Protection Laws and Regulations, Vendor shall inform ICF immediately.

3.1.3 In the event that Vendor collects Personal Data directly from individuals on behalf of ICF (or its clients), Vendor will comply with ICF's reasonable instructions to obtain required consents and provide any required notices on ICF (or its clients) behalf.

3.1.4 not Process, transfer, modify, amend, or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party, except to Authorized Sub-Processors, as required for the performance of Vendor's obligations under this DPA and the Agreement, other than in accordance with ICF's written instructions (whether in the

Agreement or otherwise) unless Processing is required by applicable Data Protection Laws and Regulations to which Vendor is subject. In the latter case, Vendor shall, to the extent permitted by such law, inform ICF of that legal requirement before Processing that Personal Data; and

3.1.5 maintain records of processing where required under Data Protection Laws and Regulations. Vendor shall assist ICF in its documentation requirements, including providing the information in a manner reasonably requested by the other party (such as using an electronic system), to enable ICF to comply with any obligations relating to maintaining records of processing.

3.2 Confidentiality and Disclosure. At all times during the term of this DPA the Vendor shall:

3.2.1 make sure that Vendor's personnel engaged in the Processing of Personal Data are informed of the confidential nature of the Personal Data, have received appropriate training on their responsibilities and have executed written confidentiality agreements.

3.2.2 make sure that such confidentiality obligations survive the termination of the personnel engagement.

3.2.3 make sure that Vendor's access to Personal Data is limited to those individuals who need access to perform Services in the context of that individual's duties to ICF.

3.2.4 not disclose or permit the disclosure of the Personal Data to any third party other than in accordance with ICF's documented instructions.

3.2.5 be permitted to disclose Personal Data as may be required by law, regulation, judicial or administrative process or in connection with litigation pertaining thereto, provided that Vendor first gives ICF prompt notice, where feasible, and a reasonable opportunity to seek an injunction to prevent the disclosure of Personal Data if ICF believes such disclosure is not legally required.

4. Return and Deletion of Personal Data

4.1 The Vendor must comply promptly with any written instructions requiring the Vendor to amend, transfer, delete or otherwise process the Personal Data or to stop, mitigate or remedy any unauthorised processing. Without prejudice to the foregoing, ICF may, at any time during the Agreement notify Vendor in writing that at no additional cost to ICF, the Vendor shall promptly (i) Delete and procure the Deletion of all copies of Personal Data Processed by Vendor or any Authorized Sub-processor; or (ii) return a complete copy of all Personal Data to ICF by secure file transfer in such format as agreed by ICF with Vendor, and Delete and procure Deletion of all other copies of Personal Data Processed by Vendor or any Authorized Sub-processor.

4.2 In the event that ICF does not give notice to the Vendor in accordance with clause 4.1, the, Vendor shall at no additional cost to ICF within ninety (90) calendar days of the Relevant Date: (i) return a complete copy of all Personal Data to ICF by secure file transfer in such format as agreed by ICF with Vendor, and Delete and procure the Deletion of all other copies of Personal Data Processed by Vendor or any Authorized Sub-processor; or (ii) Delete and procure the Deletion of all Personal Data and its copies Processed by Vendor or any Authorized Sub-processor.

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

4.4 Vendor shall, immediately upon ICF's prior written request, provide written certification to ICF that it has fully complied with the requirements of this clause 4.

5. Sub-Processing

5.1. Vendor shall not subcontract any of its processing operations performed on behalf of ICF to a Sub-processor, which include Vendor's Affiliates, without ICF's prior written authorisation, with the exception of Sub-processors currently engaged by Vendor and listed in the Annex 2 ("Authorized Sub-processors") in connection with the provision of the Services. Vendor shall submit a request for written authorisation at least 20 business days prior to the proposed engagement of a Sub-processor, together with the information necessary to enable ICF to decide on the authorisation.

5.2. At all times during the term of this DPA the Vendor shall:

5.2.1 implement adequate due diligence on each Sub-processor to ensure that it is capable of providing the level of protection for Personal Data as is required by this DPA and enter into a written agreement with each Sub-processor containing data protection obligations not less protective than those in this DPA with respect to the protection of Personal Data to the extent applicable to the nature of the Services provided by such Sub-processor. Vendor shall ensure that the Sub-processor complies with the obligations to which the processor is subject pursuant to this DPA and to Data Protection Laws and Regulations.

5.2.2 provide a copy of such a Sub-processor agreement and any subsequent amendments to ICF, immediately upon request. To the extent necessary to protect business secret or other confidential information, including Personal Data, only, the Vendor may redact the text of the agreement prior to sharing the copy.

5.2.3 maintain an up-to-date list of Authorized Sub-processors in relation to the Services and make it available to ICF upon its request.

5.2.4 remain fully liable to ICF for any failure by each Sub-processor to fulfil its obligations in relation to the Processing of any Personal Data in connection with the Services, except as otherwise set forth in the Agreement. The Vendor shall notify ICF of any failure by the Sub-processor to fulfil its contractual obligations.

5.2.5 include a clause within its Sub-processor agreements whereby in the event Vendor has factually disappeared, ceased to exist in law,has become insolvent or is otherwise incapable of performing its obligations under the AgreementICF shall have the right to instruct the Sub-processor to erase or return the Personal Data immediately upon ICF's direction.

6. International Transfers of Personal Data

6.1. Vendor shall Process Personal Data in EEA, including by using Sub-processors. Where transfers, apply Vendor shall at all times ensure that such transfers of Personal Data are made in compliance with Data Protection Laws and this Addendum.

6.2. **Restricted transfers from EEA.** This section applies solely when Processing of Personal Data by Vendor or its Authorised Sub-processors involves a transfer of EEA Personal Data to Vendor or its Authorised Sub-processors located outside of the EEA, in a Third Country.

(a.) An unmodified set of SCC, Module 2 (Controller to Processor), incorporated into this DPA as Annex 4, shall apply where ICF is a Controller, and

(b.) An unmodified set of SCC, Module 3 (Processor to Processor), incorporated into this DPA as Annex 5, shall apply where ICF is a Processor (for its clients).

6.3. **Restricted transfers from the United Kingdom**. When the Processing of Personal Data by Vendor or its Authorised Sub-processors involves a transfer subject to cross border restrictions under the UK GDPR, to Vendor or its Authorised Sub-processors outside of the United Kingdom, in a Third Country, such transfers are covered by the UK Addendum to the SCCs, incorporated as Annex 6 into this DPA.

6.4. On request from a Data Subject, ICF may make a copy of the Standard Contractual Clauses entered into between ICF and Vendor and make it available to Data Subjects.

6.5. Notwithstanding 14.5. **Order of precedence**, nothing in the Agreement shall be construed to prevail over any conflicting clause of the SCCs. For the avoidance of doubt, where this DPA further specifies audit and Sub-Processor rules, such specifications also apply in relation to the Standard Contractual Clauses insofar as these do not conflict with the Standard Contractual Clauses. To the extent the SCCs/ UK Addendum to the SCCs conflict with any provision of the Agreement

(including the DPA) the SCCs shall take precedence as it relates to EEA Personal data, and UK Addendum to the SCCs as it relates to the UK Personal Data.

6.6. Vendor shall, in relation to any Personal Data processed in connection with its obligations under this DPA:

6.6.1. Immediately notify ICF, i.e., the Data Exporter, if the Vendor, i.e., the Data Importer, is served with legally binding requests by any law enforcement or national security authority from a Third Country for disclosure of Personal Data Processed under this Appendix. In such a case, the Data Importer, in consultation with the Data Exporter, will take legal action against any such disclosure until a competent court of last resort has ordered the Data Importer to disclose the Personal Data.

6.6.2. cooperate in good faith with ICF to update this Appendix in the event that ICF determines that amendments to this Appendix are necessary following mandatory guidance or standard contractual clauses, including additional safeguards, issued by the EEA/EU and/or another relevant regulator.

6.6.3. ensure the same requirements as those in this Appendix are passed on to or otherwise required by the Vendor's Sub-processors.

6.6.4. Promptly inform ICF, if Vendor (i.) has a reason to believe that is unable to comply with any of its obligations under the Agreement, (ii.) becomes aware of circumstances or changes in Applicable Data Protection Laws that are likely to prevent it from fulfilling its obligations or changes in the in Applicable Data Protection Laws.

7. Data Protection Impact Assessment and Prior Consultation

7.1 Upon ICF's prior written request and solely in relation to Vendor's Processing of Personal Data in relation to the Services, Vendor shall assist ICF:

7.1.1 To fulfil ICF's obligation under the applicable Data Protection Laws and Regulations to implement a data protection impact assessment related to ICF's use of the Services, to the extent ICF does not otherwise have access to the relevant information.

7.1.2 in the cooperation or prior consultation with the Supervisory Authority of ICF in the performance of its tasks relating to this DPA, to the extent required under applicable Data Protection Laws and Regulations.

8. Data Subject Rights

8.1 Taking into account the nature of the Processing, Vendor, to the extent legally permitted, will:

8.1.1 promptly notify ICF if Vendor receives a request from a Data Subject to exercise the Data Subject's right of access, right to rectification, restriction of Processing, erasure/right to be forgotten, data portability, object to the Processing, right not to be subject to an automated individual decision making ("**Data Subject Request**").

8.1.2 assist ICF through the use of appropriate technical and organizational measures for the fulfilment of ICF's (or its customer, when applicable) obligation to respond to a Data Subject Request to exercise their rights under Data Protection Laws and Regulations.

9. Technical and Organisational Data Protection Standards

9.1 Vendor has implemented and will maintain appropriate administrative , technical, organizational, security and physical safeguards designed to (i) ensure the confidentiality, integrity, availability and resilience of Processing systems; (ii) protect Personal Data against any anticipated threats or hazards to confidentiality, integrity, availability and resiliency of Processing systems; and (iii) protect against accidental or unlawful loss, disclosure, alteration, unauthorized disclosure of, or access to any Personal Data transmitted, stored or otherwise Processed during the Agreement Term and as long as Personal Data is in Vendor's possession or under Vendor's control. Without limitation, Vendor shall implement and maintain the technical and organisational measures listed in Annex 2 ("Technical and Organisational Measures").

10. Audit

10.1 Upon ICF's reasonable request, Vendor shall make available to ICF all information necessary to demonstrate compliance with Vendor's obligations stemming from applicable Data Protection Laws and Regulations, and relevant with respect to Personal Data in relation to the Services (e.g., most recent third-party audits, attestations, or certifications, as applicable), within reasonable timeline, but not less than 15 (fifteen) business days.

10.2 If the copy under Section 10.1 is not acceptable for ICF's audit purposes, Vendor shall provide reasonable assistance by allowing inspection, on Vendor's premises, of relevant documents or records, to the extent such information: (i) directly relates to the transaction records for the Services provided by Vendor to ICF under the Agreement only and (ii) does not conflict with Vendor's confidentiality obligations to its other clients.

10.3 The audit shall be conducted at a mutually agreed upon time and ICF will provide Vendor with no less than ten (10) business days' advanced written notice of any requested audit. Vendor will provide appropriate management personnel to engage with ICF and supervise any audit. The onsite part of the audit shall last no longer than three (3) business days during normal business hours, unless ICF requests a longer onsite inspection period and Vendor deems it reasonable. An auditor shall not be permitted to remove any physical or electronic copies of Vendor confidential information. The Parties agree that ICF shall conduct audits in a manner that, to the extent practicable, will minimize any disruption to Vendor's business.

10.4 All information related to an audit as per this Section shall constitute confidential information of Vendor.

11. Personal Data Incident Management, Notification and Related Process.

11.1 Notification and Updates. Vendor shall notify ICF without undue delay no later than 24 hours of Vendor becoming aware of a ICF Personal Data Incident.

11.2 Investigation and Cooperation. Vendor shall make reasonable efforts to cooperate with ICF to identify the cause of such ICF Personal Data Incident and take those steps as Vendor deems necessary and reasonable to investigate and remediate the cause of such a ICF Personal Data Incident to the extent the remediation is within Vendor's reasonable control.

11.3 In the event of a ICF Personal Data Incident, Vendor shall not inform any third party without first obtaining ICF's prior written consent, unless notification is required by Data Protection Laws and Regulations or any other law to which Vendor is subject, in which case Vendor shall to the extent permitted by such law or regulation inform ICF of that legal requirement, provide a copy of the proposed notification and consider any comments made by ICF before notifying any third party of the ICF Personal Data Incident.

12. Data Protection Indemnification

12.1 Vendor shall cover all reasonable expenses associated with the performance of the obligations under the DPA unless the matter arose from ICF's specific written instructions, gross negligence or wilful default. The Vendor shall reimburse ICF for all actual reasonable expenses that ICF incurs when responding to a Data Protection Incident to the extent that the Vendor causes such incident including all costs of notice and remedy.

12.2 The Vendor agrees to indemnify, keep indemnified and defend at its own expense ICF against all costs, claims, damages or expenses incurred by ICF for which ICF may become liable due to any failure by the Vendor or its employees, subcontractors or agents to comply with any of its obligations under this DPA and/or Data Protection Laws. Vendor shall indemnify and hold harmless ICF and each ICF Affiliate against all losses, fines and sanctions arising from any claim by a third party or Supervisory Authority arising from any breach of this Addendum by the Vendor, its agents, personnel or subcontractors.

12.3 Any limitation of liability set forth in the Agreement will not apply to this DPA's indemnity or the Vendor's reimbursement obligations.

13. Warranties

13.1. The Vendor warrants and represents that:

(a) its employees and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Laws;

(b) it any anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Laws and other laws, enactments, regulations, orders, standards and other similar instruments;

(c) it has no reason to believe that the Data Protection Laws prevent it from providing any of the contracted services; and

(d) considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to the Personal Data and ensure a level of security appropriate to (i) the harm that may resolute from accident, unauthorised or unlawful processing and loss or damage; (ii) the nature of the Personal Data protected; and (iii) comply with all applicable Data Protection Laws and its information and security policies as required by this DPA.

14. General Terms

14.1 **Term and Termination**. This DPA shall remain in full force and effect so long as (a) the Agreement remains in effect; or (b) the Vendor retains any of the Personal Data related to the Agreement in its possession or control. Subject to Clause 14.2, this DPA shall terminate automatically upon, whichever is later: (i) termination of the Agreement; or (ii) expiry or termination of all service contracts, SOWs, work orders or similar contract documents entered into by Vendor with ICF and/or ICF Affiliates pursuant to the Agreement.

14.2 Any provision of this Agreement that expressly imposed on Vendor under this DPA in relation to the Processing of Personal Data shall survive any termination or expiration of this DPA.

14.3 The Vendor's failure to comply with the terms of this DPA is a material breach of the Agreement. In such event ICF may terminate the Agreement or any part of the Agreement involving the processing of Personal Data effective immediately on written notice to the Vendor without further liability or obligation of ICF.

14.4 **Governing law and Jurisdiction.** This DPA and any non-contractual rights or obligations arising out of or in connection with it shall be governed by and construed in accordance with the laws of Belgium and the courts of Belgium shall have exclusive jurisdiction to settle any disputes.

14.5 **Order of precedence**. With regard to the subject matter of this DPA, in the event of inconsistencies between the provisions of this DPA and any other agreements between the Parties, including but not limited to the Agreement, that Parties agree on the following: (a.) relevant ICF Client terms as may be incorporated into the Agreement, including in the applicable Statements of Work ("SOWs"), or in related orders forms take precedence over the provisions of this DPA; (b.) the provisions of this DPA shall take precedence over other provisions of the Agreement.

14.6 **Costs of compliance** by Vendor with the provisions of this DPA will be borne by Vendor.

14.7 **Third party rights**

14.7.1 Except to the extent set forth in governing law and in any SCCs or Binding Corporate Rules, where applicable, a person who is not a party to this DPA shall have no right to enforce any term of this DPA.

14.7.2 A ICF Affiliate may enforce any term of this DPA which is expressly or implicitly intended to benefit it. The rights of the Parties to rescind or vary this DPA are not subject to the consent of any other person.

14.8 **Severance**. Should any provision of this DPA become illegal, invalid or unenforceable in any respect under the laws of any relevant jurisdiction, then such provision shall be deemed to be severed from this DPA. Where possible, such provision shall be replaced with a lawful provision which gives effect to the intention of the Parties and, where permissible, such replacement shall not affect or impair the legality, validity or enforceability in that, or any other, jurisdiction of any other provision in this DPA.

Appendix A - Definitions.

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

1.1 "**Affiliate"** means an entity that owns or controls, is owned or controlled by or is or under common control or ownership with either Party, 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 **"Applicable Laws"** means: (a) any law, statute, directive, order, enactment, or regulation, bylaw, ordinance or subordinate legislation in force from time to time; (b) the common law and law of equity; (c) any binding court order, judgement of decree; and (d) any applicable industry code, policy or standard enforceable by law, in any jurisdiction and applicable to the Services.

1.3 **"Authorized Sub-processors"** means (a) those Subprocessors set out in **Annex 2** ("Authorized Sub-processor(s)); and (b) any additional Sub-processors authorized in writing, including by e-mail, by ICF in accordance with Section 5 ("**Subprocessing**").

1.4 "**ICF**" means ICF or ICF Affiliates, employees, representatives, Users.

1.5 **"Personal Data"** means personal data, as defined under Data Protection Laws and Regulations, described in **Annex 1** ("Details of Processing of Personal Data") and any other Personal Data Processed by Vendor or any Vendor Affiliate or its Sub-processor(s) on behalf of ICF or any ICF Affiliate pursuant to or in connection with the Agreement.

1.6 **"Data Controller"** shall have the same meaning as in the Data Protection Laws and Regulations.

1.7 **"Data Processor"** shall have the same meaning as in the Data Protection Laws and Regulations.

1.8 **"Data Protection Laws"** or "**Data Protection Laws and Regulations"** means any applicable data protection, data privacy or data security laws or electronic communications privacy laws applicable to the Processing of Personal Data under the Agreement, including but not limited to, the GDPR, Regulation (EC) 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, the Law Enforcement Directive (Directive (EU) 2016/680, UK Data Protection Bill, and any other data protection Applicable Laws within the United States, EEA and their member states, Switzerland and other jurisdictions.

1.9 **"Data Subject"**, shall have the same meaning as in the Data Protection Laws and Regulations, including but not limited to Users.

1.10 "**Delete"** means the removal or obliteration of Personal Data such that it cannot be recovered or reconstructed.

1.11 **"EEA"** means the European Economic Area.

1.12 "**EEA Personal Data**" means Personal Data that is subject to EU GDPR, such as, but not limited to, in a situation where ICF is established in the EEA.

1.13 "**EU GDPR**" means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), and any applicable national legislation adopted by the EEA member states in order to implement it into national legal order.

1.14 "**GDPR**" means the EU GDPR or the UK GDPR, as appropriate

1.15 "**ICF Personal Data**" means any Personal Data that Vendor Process on behalf of ICF pursuant to this Agreement.

1.16 **"Personal Data Breach" or** "**ICF Personal Data Incident"** means a suspected or actual breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, misuse, or access to, Personal Data transmitted, stored or otherwise Processed.

1.17 **"Process/Processing"** shall have the same meaning as in the Data Protection Laws and Regulations.

1.18 **"Relevant Date"** means the date falling on the earlier of (i) the cessation of Processing of Personal Data by Vendor or its Authorized Sub-processors; or (ii) termination of the Agreement.

1.19 **"Services"** means the Services supplied under the Agreement.

1.20 **"Standard Contractual Clauses"** or "**SCCs**" means (i) the standard contractual clauses annexed to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, as updated, amended, replaced or superseded from time to time by the European Commission; or (ii) where required from time to time by a Supervisory Authority for use with respect to any specific transfer of Personal Data to a Third Country, any other set of contractual clauses or other similar mechanism approved by such Supervisory Authority or by applicable Data Protection Laws and Regulations for use in respect of such transfer, as updated, amended, replaced or superseded from time to time by such Supervisory Authority or applicable Data Protection Laws and Regulations.

1.21 **"Sub-processor"** means any subcontracting Data Processor appointed by Data Processor to Process ICF Personal Data in the services under this Agreement

1.22 "**Supervisory Authority"** means a data protection supervisory authority which has jurisdiction over ICF, Vendor or Affiliates' (as applicable) in the Processing of Personal Data;

1.23 "**Third Country"** means the countries outside the EEA or the United Kingdom (UK), excluding countries deemed as providing adequate protection for Personal Data by the European Commission or, as appropriate, the UK Secretary of State, or the UK Information Commissioner, and approved by UK Parliament, from time to time.

1.24 "**Users**" mean customers, consumers or users of ICF services.

1.25 "**UK Addendum to the SCCs**" means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, in force 21 March 2022, as approved by UK Parliament and available at the UK ICO's webpage: https://ico.org.uk/media/for-organisations/documents/4019483/international-data-transfer-addendum.pdf.

1.26 "**UK GDPR**" means the EU GDPR as amended and incorporated into UK law under the UK European Union (Withdrawal) Act 2018, if in force.

1.27 "**UK International Data Transfer Agreement**" means the International Data Transfer Agreement, version A1.0, in force 21 March 2022, as approved by UK Parliament and available at the UK ICO's webpage: https://ico.org.uk/media/for-organisations/documents/4019538/international-data-transfer-agreement.pdf.

1.28 "**UK Personal Data**" means any Personal Data that is subject to UK GDPR, such as, but not limited to, in a situation where ICF is established in the UK.

ANNEX 1 to the DPA: DETAILS OF PROCESSING OF PERSONAL DATA

A. List of Parties:

Data exporter: ICF entity that has engaged Vendor to provide services under the Agreement
Address: as identified in the Agreement
Role: Controller or Processor as described in the DPA

Data importer: Vendor engaged to provide services under the Agreement
Address: as identified in the Agreement
Role: Processor or Sub-Processor as described in the DPA

B. Description of Processing

Purpose of the Processing: Vendor will Process Personal Data solely as necessary to perform the Services.

Duration of the Processing: Vendor will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or prohibited by law.

Categories of Data Subjects whose Personal Data is Processed: Data Subjects whose Personal Data may be Processed in relation to the Services may include, but is not limited to the following categories:

- Prospects, customers, business partners and vendors of ICF (who are natural persons)
- Employees or contact persons of ICFs prospects, customers, business partners and vendors
- Employees, agents, advisors, freelancers of ICF (who are natural persons)
- ICF's Users authorized by ICF to use the Services.

Personal Data Categories: Personal Data that may be Processed in relation to the Services, the extent of which is determined and controlled by ICF in its sole discretion, and may include, but is not limited to the following categories:

- First and last name
- Title
- Position
- Employer
- Contact information (company, email, phone, physical business address)
- Professional life data (CV, and related details)

Specific or additional Personal Data categories necessary to perform the Services as more fully described in the relevant SOW.

Sensitive data processed (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: When applicable, special categories or sensitive categories are described in the related SOW.

C. Competent Supervisory Authority for the purpose of the SCCs is in accordance with Article 13 in the SCC: Belgium.

ANNEX 2 to the DPA: TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

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

Security Controls and Safeguards

1. Security Policy and Acceptable Use Policy (AUP). Supplier will have a written Security Policy and Acceptable Use Policy that address, at a minimum, appropriate administrative, technical, organizational, security and physical safeguards outlined in this technical and organizational measures document.
2. Supplier has implemented and will maintain appropriate administrative, technical, organizational, security and physical safeguards designed to (i) ensure the confidentiality, integrity, availability and resiliency of Personal Data; (ii) protect Personal Data against any anticipated threats or hazards to confidentiality, integrity, availability and resiliency of Personal Data; and (iii) protect against any actual or suspected unauthorized processing, loss, disclosure, or acquisition of or access to any Personal Data or confidential information during the Agreement Term and as long as Client Personal Data is in Supplier's possession or under Supplier's control. Such controls include, but are not limited to:
    - 2.1.1 Data Protection and Cyber Security Awareness and Training. Supplier requires and will continue to require annual security and privacy training for all personnel with access to Client Personal Data.
    - 2.1.2 Background Checks. Supplier shall perform a criminal background check on any employee performing Supplier Services under the Agreement.
    - 2.1.3 Access Limitations. Supplier will i) limit access to its information systems and the facilities in which they are housed to authorized persons under the Agreement and to those persons who are reasonably required to know such information to perform the Services; ii) subject such authorized persons to user authentication and log on processes when they need access to Client Personal Data.; iii) the concept of least privilege is applied iv) use of strong authentication such as multi-factor or biometrics iv) store the Client Personal Data in locked facilities, storage areas or containers; and v) remove Supplier personnel access to Client Personal Data upon employment termination or a change in job status that results in the personnel no longer requiring access to Customer Personal Data.vi) have a written procedure that sets forth the manner in which Supplier restricts access to Client Personal Data;
    - 2.1.4 Password Protection. Supplier will not log passwords. Supplier will i) require strong password standards (8 characters minimum), which include length, complexity, and expiration and ii) encrypt passwords at rest and in transit iii) block access after a maximum ten (10) account attempt lockout threshold at a maximum is met. iv) passwords cannot be recycled within a specified period v) expire passwords at least every 90 days.
    - 2.1.5 Encryption. Supplier, at a minimum and where Supplier transmits Client Personal Data and communication, will use i) up to date industry-accepted encryption standards avoiding known unsafe cryptographic protocols such as SSL 3.0 and TLS 1.1 or below, to protect Client Personal Data and communications at rest and in transit.

2.1.6 Monitoring, Testing and Detection. Supplier will: i) employ an industry standard network intrusion detection system and firewalls to monitor and block suspicious network traffic; ii) reviews access logs on servers and security events and retain network security logs for 180 days; iii) review privileged access on information systems and network devices; iv) perform vulnerability assessments on a regular basis using commercially available scanning tools that identify application and operating system vulnerabilities; vi) maintain a vulnerability remediation program with reasonable SLAs; vii) ensure all endpoints run an anti-virus solution and apply timely updates; viii) maintain a patch management process that assures functional and security patches are applied in a reasonable timeframe x) maintain any software or system design, development, configuration, or implementation under the Agreement in accordance with applicable security standards and commercial industry practices; and (xi) regularly monitor network and information systems and implement and maintain security controls and procedures designed to prevent, detect and respond to identified threats and risks to reasonably calculate and prevent unauthorized access to or unauthorized use of Client Personal Data, and upgrade information safeguards as necessary to limit risks..

2.1.7 PCI-DSS Compliance. If and where applicable, Supplier shall comply, where relevant to performing Services, with the appropriate Payment Card Industry Data Security Standards.

2.1.8 Access To Contractor Systems. Where Supplier will access Client's systems, Supplier will comply with either Client's standards for third party access to Contractor systems or equivalent program standards. Written documentation of such standards and programs will be available and incorporated here by reference Supplier's access to such systems, if applicable, shall be limited to: (i) Supplier personnel who require access in order to perform Services under this Agreement; (ii) the Term of the Agreement or such other time as Client may determine in its sole discretion; and (iii) Client systems identified by Client as critical to the performance of this Agreement.

2.1.9 Remediation and Response. Supplier will document responsive actions taken regarding any data protection incident and will implement mandatory post-incident review of events and actions taken, if any, to change business practices relating to protection of Client Personal Data.

2.1.10 Business Continuity and Disaster Recovery. Supplier will i) design or has designed its solution for high availability. This includes mitigating the risk of single points of failure and providing a resilient environment to support business continuity. The solution shall include geo-diverse data storage and processing locations and infrastructures. ii) ensure disaster recovery plans are in place and test them at least once per year to validate the disaster recovery procedures and documentation

2.1.11 Backup and Reliability. Supplier will: i) configure networking components, network accelerators, load balancers, Web servers and application servers in a redundant configuration; ii) perform nightly backups of client personal data iii) store Client Personal Data on secure systems backed up in geo-diverse locations iv) encrypt backups of client personal data Secure Data Deletion. Supplier will i) observe data retention requirements of contractual agreements ii) delete client data, if requested by client iii) sanitize data storage assets in accordance with NIST SP 800-88.

ANNEX 3 to the DPA: AUTHORIZED SUBPROCESSORS

Vendor to insert Each Sub-processor's in the relevant SOW, providing the details required for Sub-processors in the table below.

#	Sub-processor's name (including Vendor's Affiliates, if applicable)	Country of Sub-processor's establishment	Countries of Processing	Purpose of Processing	DPO contact details	Transfer mechanism in place (where applicable)

ANNEX 4 to the DPA: Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries (Controller to Processor Transfers)

Standard Contractual Clauses: Module 2: Controller to Processor Transfer

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.

(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.

[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, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

Clause 3 - Third-party beneficiaries

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

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
(ii) Clause 8.1(b), 8.9(a), (c), (d) and (e);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b);

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

***Clause 4*- Interpretation**

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

***Clause 5*- Hierarchy**

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

***Clause 6* - Description of the transfer(s)**

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

***Clause 7 – Optional* - Docking clause**

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

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligatios 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 TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

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

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

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

8.9 Documentation and compliance

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

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

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

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

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

***Clause 9* - Use of sub-processors**

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least 20 (twenty) business days prior to the engagement of the sub-processor, together with

[2] 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.

the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

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

Clause 11 - Redress

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

(i) The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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

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

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12 – Liability

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

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

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

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

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

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

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

Clause 13 – Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

[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

(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[3];

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

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

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

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

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

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

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

[3] 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.

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

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

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

Clause 17 - Governing law

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

Clause 18 - Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of Belgium (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE SCCS: See Annex 1 of the DPA.

ANNEX II TO THE SCCS: See Annex 2 of the DPA.

ANNEX II TO THE SCCS: See Annex 3 of the DPA.

ANNEX 5 to the DPA: Standard Contractual Clauses for the Transfer of Personal Data from the EU to Third Countries

Module 3: Processor to Processor Transfers

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)[4] for the transfer of personal data to a third country.

(b) The Parties:

(iii) 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

(iv) 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 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g);
(iii) Clause 9(a), (c), (d) and (e);
(iv) Clause 12(a), (d) and (f);
(v) Clause 13;
(vi) Clause 15.1(c), (d) and (e);
(vii) Clause 16(e);
(viii) Clause 18(a) and (b);

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

Clause 4 – Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

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

(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 THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter[5].

[5] See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

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 controller, as communicated to the data importer by the data exporter, or 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 personal data, the data exporter 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.

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 rectify or erase 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 controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing
(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, 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. 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 or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller 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 data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide

all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn 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 set out 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 controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union[6] (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 of Regulation (EU) 2016/679;

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

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

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

8.9 Documentation and compliance

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

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

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

[6] 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 purposes of these Clauses.

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

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

Clause 9 - Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the prior specific written authorisation of the controller. The data importer shall submit the request for specific authorisation at least 20 (twenty) prior to the engagement of the sub-processor, together with the information necessary to enable the controller to decide on the authorisation. It shall inform the data exporter of such engagement. The list of sub-processors already authorised by the controller can be found in Annex III. The Parties shall keep Annex III up to date.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), 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[7]. The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 - Data subject rights

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.
(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.
(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

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

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.

(i) The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.

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

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

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
(ii) refer the dispute to the competent courts within the meaning of Clause 18.

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

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

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

Clause 12 – Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.
(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.
(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.
(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.
(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.
(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.
(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 – Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

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

[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

(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[8];

[8] 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

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

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

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

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

(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, if appropriate in consultation with the controller. 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 controller or the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 - Obligations of the data importer in case of access by public authorities

15.1 Notification

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

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

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

The data exporter shall forward the notification to the controller.

(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.

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.

(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.). The data exporter shall forward the information to the controller.

(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. The data exporter shall make the assessment available to the controller.

(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 and the controller of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

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

Clause 17 - Governing law

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

Clause 18 - Choice of forum and jurisdiction

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

(b) The Parties agree that those shall be the courts of [Belgium]_____ (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE SCCS: See Annex 1 of the DPA.

ANNEX II TO THE SCCS: See Annex 2 of the DPA.

ANNEX II TO THE SCCS: See Annex 3 of the DPA.

ANNEX 6 to the DPA - 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.

1.29 Part 1: Tables

1.29.1 Table 1: Parties

Start date	In accordance with Article 3.1 of the IGDTA.	
The Parties	**Exporter (who sends the Restricted Transfer)**	**Importer (who receives the Restricted Transfer)**
Parties' details	See Annex 1 of the DPA.	See Annex 1 of the DPA.
Key Contact	See Annex 1 of the DPA.	See Annex 1 of the DPA.
Signature (if required for the purposes of Section 2)		

1.29.2 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: Date: See the date of the Agreement/ DPA Reference (if any): The Agreement, including the DPA Other identifier (if any): Or ☐ the Approved EU SCCs, including the Appendix Information and with only the following modules, clauses or optional provisions of the Approved EU SCCs brought into effect for the purposes of this Addendum:					
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						

1.29.3 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: See "Schedule A-I - Parties to the Agreement" to the Intra-group Data Protection Agreement, and any Participation Agreement, if applicable.
Annex 1B: Description of Transfer: See Schedule B Description of the Processing to the Intra-group Data Protection Agreement.
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II to Schedules C, D, E to the Intra-group Data Protection Agreement.
Annex III: List of Sub processors (Modules 2 and 3 only)

1.29.4 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: ☒ Importer ☒ Exporter ☐ neither Party

1.30 Part 2: Mandatory Clauses

1.30.1 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.

1.30.2 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.

1.30.3 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.

1.30.4 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.

1.30.5 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.

1.31 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.