

OFFICIAL-SENSITIVE (COMMERCIAL)

SCHEDULE 11

PROCESSING PERSONAL DATA

1 Processing Personal Data

- 1.1 This Schedule supplements Clause 19 (*Protection of Personal Data*) of this Agreement and should be read and interpreted alongside those provisions.
- 1.2 All data processing activities shall comply with the Joint Recruiting Data Protection Policy (published by the Authority, as updated from time to time (the latest iteration of which, at the time of the signing of this Agreement, is appended to Annex 4 (*Joint Recruiting Data Protection Policy*))).
- 1.3 DEFCON 532B shall apply to this Agreement.
- 1.4 The contact details of the Authority's Data Protection Officer are: **[Insert Contact details]** and contact details of the relevant Data Protection Advisor are **[Insert contact details]**.
- 1.5 The contact details of the Supplier's Data Protection Officer are: **[Insert Contact details]**
- 1.6 The Processor shall comply with any further written instructions with respect to processing by the Controller.
- 1.7 Any such further instructions shall be incorporated into this Schedule.
- [Note to Bidders: the parties shall work together prior to finalising the Agreement to ensure the information about the processing below is accurate]**
- 1.8 The table below sets out the basis of the processing applicable to this Agreement. In completing the information required, the Authority may take account of the view of the Supplier, however the final decision as to the content (including any updates after the Effective Date) shall be at the Authority's at its absolute discretion.

Description	Details
Identity of Controller and Processor for each Category of Personal Data	<p>The Authority is Controller and the Supplier is Processor</p> <p>The Parties acknowledge that in accordance with Clause 18 and for the purposes of the Data Protection Legislation, the Authority is the Controller and the Supplier is the Processor of the following Personal Data:</p> <ul style="list-style-type: none"> [Insert the scope of Personal Data for which the purposes and means of the processing by the Supplier is determined by the Authority] <p>The Supplier is Controller and the Authority is Processor</p> <p><i>The Parties acknowledge that for the purposes of the Data Protection Legislation, the Supplier is the Controller and the Authority is the Processor in accordance with Clause 18 of the following Personal Data:</i></p>

OFFICIAL-SENSITIVE (COMMERCIAL)

	<ul style="list-style-type: none"> • [Insert the scope of Personal Data for which the purposes and means of the processing by the Authority is determined by the Supplier] <p>The Parties are Joint Controllers</p> <p><i>The Parties acknowledge that they are Joint Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none"> • [Insert the scope of Personal Data for which the purposes and means of the processing is determined by both Parties together] <p>The Parties are Independent Controllers of Personal Data</p> <p><i>The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of:</i></p> <ul style="list-style-type: none"> • <i>Business contact details of Supplier Personnel,</i> • <i>Business contact details of any directors, officers, employees, agents, consultants and contractors of the Authority (excluding the Supplier Personnel) engaged in the performance of the Authority's duties under this Agreement).</i> • [Insert the scope of other Personal Data provided by one Party who is Data Controller to the other Party who will separately determine the nature and purposes of its processing the Personal Data on receipt e.g. where (1) the Supplier has professional or regulatory obligations in respect of Personal Data received, (2) a standardised service is such that the Authority cannot dictate the way in which Personal Data is processed by the Supplier, or (3) where the Supplier comes to the transaction with Personal Data for which it is already Controller for use by the Authority]
Data Subjects / Categories of Data Subject	[Examples include: Staff (including volunteers, agents, and temporary workers), customers/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]
Type of personal data	[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]
Nature and purposes of the processing (Processing operations activities) /	<p>[Please be as specific as possible, but make sure that you cover all intended purposes.</p> <p><i>The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc.</i></p> <p><i>The purpose might include: employment processing, statutory obligation, recruitment assessment etc]</i></p>

OFFICIAL-SENSITIVE (COMMERCIAL)

Special Technical and Organisational Measures (to safeguard data)	
Instructions for Disposal of Personal Data once the processing is complete	<i>[Describe how data will be destroyed, or alternatively how it be returned, if that it is the instruction]</i>
Date from which Personal Data is to be Processed	
Duration of the Processing	<i>[Clearly set out the duration of the processing including dates]</i>

ANNEX 1: JOINT CONTROLLER AGREEMENT

1 Joint Controller Status and Allocation of Responsibilities

1.1 With respect to Personal Data under Joint Control of the Parties, the Parties envisage that they shall each be a Data Controller in respect of that Personal Data in accordance with the terms of this Annex 1 (*Joint Controller Agreement*) in replacement of Clause 19.2-19.15 (Where one Party is Controller and the other Party is Processor) and 19.17-19.27 (Independent Controllers of Personal Data). Accordingly, the Parties each undertake to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Data Controllers.

1.2 The Parties agree that the **[Supplier/Authority]:**

- (a) is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the GDPR regarding the exercise by Data Subjects of their rights under the GDPR;
- (b) shall direct Data Subjects to its Data Protection Officer or suitable alternative in connection with the exercise of their rights as Data Subjects and for any enquiries concerning their Personal Data or privacy;
- (c) is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the GDPR;
- (d) is responsible for obtaining the informed consent of Data Subjects, in accordance with the GDPR, for Processing in connection with the Services where consent is the relevant legal basis for that Processing; and
- (e) shall make available to Data Subjects the essence of this Joint Controller Agreement (and notify them of any changes to it) concerning the allocation of responsibilities as Joint Controller and its role as exclusive point of contact, the Parties having used their best endeavours to agree the terms of that essence. This must be outlined in the Supplier's privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing) which shall align with the Joint Recruiting Data Protection Policy.

1.3 Notwithstanding the terms of Paragraph 1.1, the Parties acknowledge that a Data Subject has the right to exercise their legal rights under the Data Protection Legislation as against the relevant Party as Data Controller.

2 Undertakings of both Parties

2.1 The Supplier and the Authority each undertake that they shall:

- ~~(a)~~ (a) report to the other Party quarterly (on dates to align with the Authority's reporting cycles):
 - (i) the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

OFFICIAL-SENSITIVE (COMMERCIAL)

- (ii) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;
- (iii) any other requests, complaints or communications from Data Subjects (or third parties on their behalf) relating to the other Party's obligations under applicable Data Protection Legislation;
- (iv) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and
- (v) any requests from any third party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law;

that it has received in relation to the subject matter of the Agreement during that period;

- (b) notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1(a)(i) to (a)(v); and
- (c) provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 2.1(a)(i) to (a)(v) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation.
- (d) not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and, for any disclosure or transfer of Personal Data to any third party, save where such disclosure or transfer is specifically authorised under this Agreement or is required by Law). For the avoidance of doubt to which Personal Data is transferred must be subject to equivalent obligations which are no less onerous than those set out in this Annex 1 (*Joint Controller Agreement*).
- (e) request from the Data Subject only the minimum information necessary to provide the Services and treat such extracted information as Confidential Information.
- (f) ensure that at all times it has in place appropriate Protective Measures to guard against unauthorised or unlawful processing of the Personal Data and/or accidental loss, destruction or damage to the Personal Data and unauthorised or unlawful disclosure of or access to the Personal Data
- (g) take all reasonable steps to ensure the reliability and integrity of any of its Personnel who have access to the Personal Data and ensure that its Personnel:
 - (i) are aware of and comply with their duties under this Annex 1 (*Joint Controller Agreement*) and those in respect of Confidential Information
 - (ii) are informed of the confidential nature of the Personal Data, are subject to appropriate obligations of confidentiality and do not publish, disclose or divulge any of the Personal Data to any third party where the that Party would not be permitted to do so;

OFFICIAL-SENSITIVE (COMMERCIAL)

- (iii) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;
 - (h) ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Data Loss Event;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures.
 - (i) ensure that it has the capability (whether technological or otherwise), to the extent required by Data Protection Legislation, to provide or correct or delete at the request of a Data Subject all the Personal Data relating to that Data Subject that the Supplier holds; and
 - (j) ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event.
- 2.2 Each Joint Controller shall use its reasonable endeavours to assist the other Controller to comply with any obligations under applicable Data Protection Legislation and shall not perform its obligations under this Annex 1 (*Joint Controller Agreement*) in such a way as to cause the other Joint Controller to breach any of its' obligations under applicable Data Protection Legislation to the extent it is aware, or ought reasonably to have been aware, that the same would be a breach of such obligations
- 3 Data Protection Breach**
- 3.1 Without prejudice to Paragraph 3.2 and 3.3, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Personal Data Breach or circumstances that are likely to give rise to a Personal Data Breach, providing the other Party and its advisors with:
- (a) sufficient information and in a timescale which allows the other Party to meet any obligations to report a Personal Data Breach under the Data Protection Legislation;
 - (b) all reasonable assistance, including:
 - (i) co-operation with the other Party and the Information Commissioner investigating the Personal Data Breach and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;
 - (ii) co-operation with the other Party including taking such reasonable steps as are directed by the Authority to assist in the investigation, mitigation and remediation of a Personal Data Breach;

OFFICIAL-SENSITIVE (COMMERCIAL)

- (iii) co-ordination with the other Party regarding the management of public relations and public statements relating to the Personal Data Breach;
 - (iv) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Personal Data Breach, with complete information relating to the Personal Data Breach, including, without limitation, the information set out in Paragraph 3.2.
- 3.2 In relation to data security incidents, the parties shall comply with any requirements and timeframes imposed by the Authority's warning and reporting point (WARP) and/or the Data Protection Support Team.
- 3.3 Each Party shall take all steps to restore, re-constitute and/or reconstruct any Personal Data where it has lost, damaged, destroyed, altered or corrupted as a result of a Personal Data Breach as if it was that Party's own data at its own cost with all possible speed and shall provide the other Party with all reasonable assistance in respect of any such Personal Data Breach, including providing the other Party, as soon as possible and within forty-eight (48) hours of the Personal Data Breach relating to the Personal Data Breach, in particular:
 - (a) the nature of the Personal Data Breach;
 - (b) the nature of Personal Data affected;
 - (c) the categories and number of Data Subjects concerned;
 - (d) the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;
 - (e) measures taken or proposed to be taken to address the Personal Data Breach; and
 - (f) describe the likely consequences of the Personal Data Breach.

4 Audit

- 4.1 The Supplier shall permit:
 - (a) the Authority, or a third-party auditor acting under the Authority's direction, to conduct, at the Authority's cost, data privacy and security audits, assessments and inspections concerning the Supplier's data security and privacy procedures relating to Personal Data, its compliance with this Annex 1 (*Joint Controller Agreement*) and the Data Protection Legislation.
 - (b) the Authority, or a third-party auditor acting under the Authority's direction, access to premises at which the Personal Data is accessible or at which it is able to inspect any relevant records, including the record maintained under Article 30 GDPR by the Supplier so far as relevant to the Agreement, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services.

- 4.2 The Authority may, in its sole discretion, require the Supplier to provide evidence of the Supplier's compliance with Paragraph 4.1 in lieu of conducting such an audit, assessment or inspection.

5 Impact Assessments

- 5.1 The Parties shall:

- (a) provide all reasonable assistance to each other to prepare any Data Protection Impact Assessment as may be required (including provision of detailed information and assessments in relation to processing operations, risks and measures);
- (b) maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with this Agreement, in accordance with the terms of Article 30 GDPR.

6 ICO Guidance

The Parties agree to take account of any guidance issued by the Information Commissioner and/or any relevant Central Government Body. The Authority may on not less than thirty (30) Working Days' notice to the Supplier amend this Agreement to ensure that it complies with any guidance issued by the Information Commissioner and/or any relevant Central Government Body.

7 Liabilities for Data Protection Breach

- 7.1 If financial penalties are imposed by the Information Commissioner on either the Authority or the Supplier for a Personal Data Breach ("**Financial Penalties**") then the following shall occur:

- (a) If in the view of the Information Commissioner, the Authority is responsible for the Personal Data Breach, in that it is caused as a result of the actions or inaction of the Authority, its employees, agents, contractors (other than the Supplier) or systems and procedures controlled by the Authority, then the Authority shall be responsible for the payment of such Financial Penalties. In this case, the Authority will conduct an internal audit and engage at its reasonable cost when necessary, an independent third party to conduct an audit of any such data incident. The Supplier shall provide to the Authority and its third party investigators and auditors, on request and at the Supplier's reasonable cost, full cooperation and access to conduct a thorough audit of such data incident;
- (b) If in the view of the Information Commissioner, the Supplier is responsible for the Personal Data Breach, in that it is not a breach that the Authority is responsible for, then the Supplier shall be responsible for the payment of these Financial Penalties. The Supplier will provide to the Authority and its auditors, on request and at the Contractor's sole cost, full cooperation and access to conduct a thorough audit of such data incident.

OFFICIAL-SENSITIVE (COMMERCIAL)

- (c) If no view as to responsibility is expressed by the Information Commissioner, then the Authority and the Supplier shall work together to investigate the relevant data incident and allocate responsibility for any Financial Penalties as outlined above, or by agreement to split any financial penalties equally if no responsibility for the Personal Data Breach can be apportioned. In the event that the Parties do not agree such apportionment then such Dispute shall be referred to the Dispute Resolution Procedure set out in Schedule 8.3 (*Dispute Resolution Procedure*).
- 7.2 If either the Authority or the Supplier is the defendant in a legal claim brought before a court of competent jurisdiction (“**Court**”) by a third party in respect of a Personal Data Breach, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Personal Data Breach shall be liable for the losses arising from such breach. Where both Parties are liable, the liability will be apportioned between the Parties in accordance with the decision of the Court.
- 7.3 In respect of any losses, cost claims or expenses incurred by either Party as a result of a Personal Data Breach (the “**Claim Losses**”):
 - (a) if the Authority is responsible for the relevant breach, then the Authority shall be responsible for the Claim Losses;
 - (b) if the Supplier is responsible for the relevant breach, then the Supplier shall be responsible for the Claim Losses: and
 - (c) if responsibility is unclear, then the Authority and the Supplier shall be responsible for the Claim Losses equally.
- 7.4 Nothing in Paragraphs 7.2-7.3 shall preclude the Authority and the Supplier reaching any other agreement, including by way of compromise with a third party complainant or claimant, as to the apportionment of financial responsibility for any Claim Losses as a result of a Personal Data Breach, having regard to all the circumstances of the breach and the legal and financial obligations of the Authority.

8 Termination

If the Supplier is in material Default under any of its obligations under this Annex 1 (*Joint Control Agreement*), the Authority shall be entitled to terminate this Agreement by issuing a Termination Notice to the Supplier in accordance with Clause 29 (*Termination Rights*).

9 Sub-Processing

- 9.1 In respect of any Processing of Personal performed by a third party on behalf of a Party, that Party shall:
 - (a) carry out adequate due diligence on such third party to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Agreement, and provide evidence of such due diligence to the other Party where reasonably requested; and

- (b) ensure that a suitable agreement is in place with the third party as required under applicable Data Protection Legislation.

10 Data Retention

The Parties agree to erase Personal Data from any computers, storage devices and storage media that are to be retained as soon as practicable after it has ceased to be necessary for them to retain such Personal Data under applicable Data Protection Legislation and in accordance with the Joint Recruiting Data Protection Policy (save to the extent (and for the limited period) that such information needs to be retained by a Party for statutory compliance purposes or as otherwise required by this Agreement), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and the Joint Recruiting Data Protection Policy.

ANNEX 2: CONTROLLER TO CONTROLLER STANDARD CONTRACTUAL CLAUSES

[Note to Bidders: Annexes 2 and 3 were added to the MSC on the recent update and seek to address the current situation with regards to data transfers following Brexit. Given this, this Schedule 11 and these Annexes (and the corresponding Clause 19 of the Agreement) may be subject to further amendment]

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers) Data transfer agreement between

(name)

(address and country of establishment)

hereinafter “data exporter”)

and

(name)

(address and country of establishment)

hereinafter “data importer”, and

each a “party”; together “the parties”.

Definitions

For the purposes of the clauses:

- (A) “personal data”, “special categories of data/sensitive data”, “process/processing”, “controller”, “processor”, “data subject” and “supervisory authority/authority” shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby “the authority” shall mean the competent data protection authority in the territory in which the data exporter is established);
- (B) “the data exporter” shall mean the controller who transfers the personal data;
- (C) “the data importer” shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country’s system ensuring adequate protection;
- (D) “clauses” shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.
- (E) The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

Obligations of the data exporter

The data exporter warrants and undertakes that:

- a) The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.
- b) It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.
- c) It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.
- d) It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.
- e) It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II. Obligations of the data importer

The data importer warrants and undertakes that:

- a) It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.
- b) It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain

OFFICIAL–SENSITIVE (COMMERCIAL)

the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

- c) It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.
- d) It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.
- e) It will identify to the data exporter a contact point within its organization authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).
- f) At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).
- g) Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.
- h) It will process the personal data, at its option, in accordance with:

OFFICIAL-SENSITIVE (COMMERCIAL)

- (i) the data protection laws of the country in which the data exporter is established; or
- (ii) the relevant provisions of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data; or
- (iii) the data processing principles set forth in Annex A.

Data importer to indicate which option it selects:

Initials of data importer: _____;

- i) It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer, and:
 - (i) the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection; or
 - (ii) the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU; or
 - (iii) data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards; or
 - (iv) with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer.

III. Liability and third party rights

- a) Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damages suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

- b) The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV. Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V. Resolution of disputes with data subjects or the authority

- j) In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.
- k) The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.
- l) Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI. Termination

- a) In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

OFFICIAL-SENSITIVE (COMMERCIAL)

b) In the event that:

- (i) the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a) above;
- (ii) compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;
- (iii) the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;
- (iv) a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or
- (v) a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

Signed:

Date:

FOR DATA IMPORTER

Signed:

Date:

FOR DATA EXPORTER

ANNEX A

DATA PROCESSING PRINCIPLES

- 1) Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.
- 2) Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.
- 3) Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.
- 4) Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.
- 5) Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation.

OFFICIAL-SENSITIVE (COMMERCIAL)

The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

- 6) Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.
- 7) Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to “opt-out” from having his data used for such purposes.
- 8) Automated decisions: For purposes hereof “automated decision” shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:
 - a) (i) such decisions are made by the data importer in entering into or performing a contract with the data subject; and

(ii) (the data subject is given an opportunity to discuss the results of a relevant automated decision with a representative of the parties making such decision or otherwise to make representations to that parties;
 - Or
 - b) where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

(To be completed by the parties)

Data Subjects

The personal data transferred concern the following categories of data subjects:

Purposes of the transfer(s)

The transfer is made for the following purposes:

Categories of data

The personal data transferred concern the following categories of data :

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

Sensitive data (if appropriate)

The personal data transferred concern the following categories of sensitive data:

Data protection registration information of data exporter (where applicable):

Additional use information (storage limits and other relevant information):

Contact points for data protection enquiries:

Data importer

Data Exporter

ANNEX 3: CONTROLLER TO PROCESSOR STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Tel. ; fax ; e-mail:

Other information needed to identify the organisation

(the data **exporter**)

And

Name of the data importing organisation:

Address:

Tel. ; fax ; e-mail:

Other information needed to identify the organisation

(the data **importer**)

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

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

OFFICIAL–SENSITIVE (COMMERCIAL)

Clause 1

Definitions

For the purposes of the Clauses:

- a) ‘personal data’, ‘special categories of data’, ‘process/processing’, ‘controller’, ‘processor’, ‘data subject’ and ‘supervisory authority’ shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data³;
- b) ‘the data exporter’ means the controller who transfers the personal data;
- c) ‘the data importer’ means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country’s system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- d) ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- e) ‘the applicable data protection law’ means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;
- f) ‘technical and organisational security measures’ means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

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

Clause 3

Third-party beneficiary clause

- (a) The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
- (b) The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
- (c) The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
- (d) The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

- a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred

OFFICIAL-SENSITIVE (COMMERCIAL)

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

- c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
- d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- e) that it will ensure compliance with the security measures;
- f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;
 - (ii) any accidental or unauthorised access; and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

OFFICIAL-SENSITIVE (COMMERCIAL)

- g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;
- h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
- i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;
- j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6 Liability

- a) The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
- b) If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.
- c) The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.
- d) If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data

OFFICIAL–SENSITIVE (COMMERCIAL)

importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

- a) The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (i) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (ii) to refer the dispute to the courts in the Member State in which the data exporter is established.
- b) 2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

- a) The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
- b) The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
- c) The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

OFFICIAL-SENSITIVE (COMMERCIAL)

Clause 9

Governing law

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

Clause 10

Variation of the contract

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

Clause 11

Sub-processing

- a) The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.
- b) The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.
- c) The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely.....

OFFICIAL-SENSITIVE (COMMERCIAL)

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

Clause 12

Obligation after the termination of personal data-processing services

- (a) The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
- (b) The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

Signed:

Signed:

Date:

Date:

FOR DATA IMPORTER

FOR DATA EXPORTER

[insert stamp of organisation]

[insert stamp of organisation]

Appendix 1
to the Standard Contractual Clauses

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

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is (please specify the activities relevant to transfer):

Data importer

The data importer is (please specify the activities relevant to transfer):

Data subjects

The personal data transferred concern the following categories of data subjects:

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

Processing operations

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

Signed:

Date:

Signed:

Date:

FOR DATA IMPORTER

[insert stamp of organisation]

FOR DATA EXPORTER

[insert stamp of organisation]

Appendix 2
to the Standard Contractual Clauses

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

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

ANNEX 4: JOINT RECRUITING DATA PROTECTION POLICY

In accordance with this Schedule 11, the Supplier shall at all times comply with the Joint Recruiting Data Protection Policy published by the Authority (as updated from time to time).

The latest iteration of the Joint Recruiting Data Protection Policy, at the time of the signing of this Agreement, is appended below.



20200305-JRDPP_G
DPR_V2.docx