CONTRACT FOR PRISONER AND NON-PRISONER FOOD SUPPLY

SCHEDULE 31

PROCESSING PERSONAL DATA

1 DATA PROCESSING

1.1 This Schedule shall be completed by the Controller, who may take account of the view of the Processor, however the final decision as to the content of this Schedule shall be with the Authority at its absolute discretion.

1.2 The contact details of the Authority's Data Protection Officer are: **The text has been redacted under the exemptions set out by the Freedom of Information Act**

1.3 The contact details of the Supplier's Data Protection Officer are: **The text has been redacted under the exemptions set out by the Freedom of Information Act**

1.4 The Processor shall comply with any further written instructions with respect to processing by the Controller.

1.5 Any such further instructions shall be incorporated into this Schedule.

Description	Details
Identity of Controller for each Category of Personal Data	**The Authority is Controller and the Supplier is Processor** The Parties acknowledge that in accordance with Clauses 26.2 to 26.19 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: • Any Personal Data contained in the Authority Data. **The Parties are Independent Controllers of Personal Data** The Parties acknowledge that they are Independent Controllers for the purposes of the Data Protection Legislation in respect of: • Personally identifiable information of Supplier Personnel. • Personally identifiable information 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).
Subject matter of the Processing	The processing is needed in order to ensure that the Supplier and the Authority can effectively meet their obligations under the Agreement to provide the Services as detailed in the Agreement.
Duration of the processing	Processing will be required for the duration of the Agreement and until return or deletion has been completed at the end of the Term or Termination. Return or deletion requirements will be confirmed by the Authority prior to the end of the Term or Termination.
Nature and purposes of the processing	The nature of the processing means any operation required to meet a party's obligations under the Agreement including, but not limited to, 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).

Description	Details
	The purpose includes processing Authority Data to be able to provide the Services under the Agreement (i.e. on the basis of a contract).
Type of Personal Data being processed	Any Personal Data contained in the Authority Data. Examples include information about individuals working in the prisons, such as name, job title, email address and telephone number.
Categories of Data Subject	Individuals working in the prisons.
Plan for return and destruction of the data once the processing is complete UNLESS requirement under law to preserve that type of data	Authority Data will be returned or deleted at the end of the Term or Termination. Instructions will be provided by the Authority prior to the end of the Term or Termination.
Locations at which the Supplier and/or its Sub-contractors process Personal Data under this Contract and international transfers and legal gateway	UK only.

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 26.3 – 26.19 (*Where one Party is Controller and the other Party is Processor*) and 26.21 – 26.31 (*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]:

1.2.1 is the exclusive point of contact for Data Subjects and is responsible for all steps necessary to comply with the UK GDPR regarding the exercise by Data Subjects of their rights under the UK GDPR;

1.2.2 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;

1.2.3 is solely responsible for the Parties' compliance with all duties to provide information to Data Subjects under Articles 13 and 14 of the UK GDPR;

1.2.4 is responsible for obtaining the informed consent of Data Subjects, in accordance with the UK GDPR, for Processing in connection with the Services and supply of the Products where consent is the relevant legal basis for that Processing; and

1.2.5 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/Authority's] privacy policy (which must be readily available by hyperlink or otherwise on all of its public facing services and marketing).

1.3 Notwithstanding the terms of Paragraph 1.2, 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:

2.1.1 report to the other Party every [x] months on:

(a) the volume of Data Subject Access Requests (or purported Data Subject Access Requests) from Data Subjects (or third parties on their behalf);

(b) the volume of requests from Data Subjects (or third parties on their behalf) to rectify, block or erase any Personal Data;

(c) 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;

(d) any communications from the Information Commissioner or any other regulatory authority in connection with Personal Data; and

(e) 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 Contract during that period;

2.1.2 notify each other immediately if it receives any request, complaint or communication made as referred to in Paragraphs 2.1.1 to (e); and

2.1.3 provide the other Party with full cooperation and assistance in relation to any request, complaint or communication made as referred to in Paragraphs 1.2 and 2.1.1(c) to (e) to enable the other Party to comply with the relevant timescales set out in the Data Protection Legislation.

2.1.4 not disclose or transfer the Personal Data to any third party unless necessary for the provision of the Services and supply of the Products and, for any disclosure or transfer of Personal Data to any third party, (save where such disclosure or transfer is specifically authorised under this Contract or is required by Law) that disclosure or transfer of Personal Data is otherwise considered to be lawful processing of that Personal Data in accordance with Article 6 of the UK GDPR or EU GDPR (as the context requires). 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.

2.1.5 request from the Data Subject only the minimum information necessary to provide the Services and supply the Products and treat such extracted information as Confidential Information.

2.1.6 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

2.1.7 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:

(a) are aware of and comply with their duties under this Annex 1 (*Joint Controller Agreement*) and those in respect of Confidential Information

(b) 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 that Party would not be permitted to do so;

(c) have undergone adequate training in the use, care, protection and handling of personal data as required by the applicable Data Protection Legislation;

2.1.8 ensure that it has in place Protective Measures as appropriate to protect against a Data Loss Event having taken account of the:

(a) nature of the data to be protected;

(b) harm that might result from a Data Loss Event;

(c) state of technological development; and

(d) cost of implementing any measures.

2.1.9 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;

2.1.10 ensure that it notifies the other Party as soon as it becomes aware of a Data Loss Event;

2.1.11 not transfer such Personal Data outside of the UK and/or the EEA unless the prior written consent of the non-transferring Party has been obtained, and the following conditions are fulfilled:

(a) the destination country has been recognised as adequate by the UK government is in accordance with Article 45 of the UK GDPR or DPA 2018 Section 74A and/or the transfer is in accordance with Article 45 of the EU GDPR (where applicable); or

(b) the transferring Party has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the UK GDPR or DPA 2018 Section 75 and/or Article 46 of the EU GDPR (where applicable) as agreed with the non-transferring Party which could include the International Data Transfer Agreement or International Data Transfer Agreement Addendum to the European Commission's SCCs as published by the Information Commissioner's Office (as appropriate), as well as any additional measures;

(A) where the transfer is subject to UK GDPR:

(i) the UK International Data Transfer Agreement (the "**IDTA**") as published by the Information Commissioner's Office [or such updated version of such IDTA as is published by the Information Commissioner's Office under section 119A(1) of the DPA 2018 from time to time]; or

(ii) the European Commission's Standard Contractual Clauses per decision 2021/914/EU [or such updated version of such Standard Contractual Clauses as are published by the European Commission from time to time] (the "**EU SCCs**"), together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**"); and/or

(B) where the transfer is subject to EU GDPR, the EU SCCs,

(as well as any additional measures determined by the Controller being implemented by the importing party;

(c) the Data Subject has enforceable rights and effective legal remedies;

(d) the transferring Party complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the non-transferring Party in meeting its obligations); and

(e) the transferring Party complies with any reasonable instructions notified to it in advance by the non-transferring Party with respect to the processing of the Personal Data; and

2.2 Each Joint Controller shall use its best 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 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, each Party shall notify the other Party promptly and without undue delay, and in any event within 48 hours, upon becoming aware of any Data Loss Event or circumstances that are likely to give rise to a Data Loss Event, providing the other Party and its advisors with:

3.1.1 sufficient information and in a timescale which allows the other Party to meet any obligations to report a Data Loss Event under the Data Protection Legislation;

3.1.2 all reasonable assistance, including:

(a) co-operation with the other Party and the Information Commissioner investigating the Data Loss Event and its cause, containing and recovering the compromised Personal Data and compliance with the applicable guidance;

(b) 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 Data Loss Event;

(c) co-ordination with the other Party regarding the management of public relations and public statements relating to the Data Loss Event;

(d) providing the other Party and to the extent instructed by the other Party to do so, and/or the Information Commissioner investigating the Data Loss Event, with complete information relating to the Data Loss Event, including, without limitation, the information set out in Paragraph 3.2.

3.2 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 Data Loss Event which is the fault of that Party, 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 Data Loss Event, including providing the other Party, as soon as possible and within 48 hours of the Data Loss Event relating to the Data Loss Event, in particular:

3.2.1 the nature of the Data Loss Event;

3.2.2 the nature of Personal Data affected;

3.2.3 the categories and number of Data Subjects concerned;

3.2.4 the name and contact details of the Supplier's Data Protection Officer or other relevant contact from whom more information may be obtained;

3.2.5 measures taken or proposed to be taken to address the Data Loss Event; and

3.2.6 describe the likely consequences of the Data Loss Event.

4. Audit

4.1 The Supplier shall permit:

4.1.1 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 and the Data Protection Legislation.

4.1.2 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 of the UK GDPR by the Supplier so far as relevant to the Contract, and procedures, including premises under the control of any third party appointed by the Supplier to assist in the provision of the Services and supply of the Products.

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:

5.1.1 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);

5.1.2 maintain full and complete records of all Processing carried out in respect of the Personal Data in connection with this Contract, in accordance with the terms of Article 30 of the UK GDPR.

6. ICO Guidance

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

7. Liabilities for Data Protection Breach

[Guidance note: This paragraph represents a risk share, you may wish to reconsider the apportionment of liability and whether recoverability of losses are likely to be hindered by the contractual limitation of liability provisions.]

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

7.1.1 If in the view of the Information Commissioner, the Authority is responsible for the Data Loss Event, 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;

7.1.2 If in the view of the Information Commissioner, the Supplier is responsible for the Data Loss Event, 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 Supplier's sole cost, full cooperation and access to conduct a thorough audit of such data incident; or

7.1.3 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 Data Loss Event 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 23 (*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 Data Loss Event, then unless the Parties otherwise agree, the Party that is determined by the final decision of the court to be responsible for the Data Loss Event 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 Data Loss Event (the "**Claim Losses**"):

7.3.1 if the Authority is responsible for the relevant breach, then the Authority shall be responsible for the Claim Losses;

7.3.2 if the Supplier is responsible for the relevant breach, then the Supplier shall be responsible for the Claim Losses; and

7.3.3 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 Data Loss Event, having regard to all the circumstances of the breach and the legal and financial obligations of the Authority.

8. Termination

8.1 If the Supplier is in material Default under any of its obligations under this Annex 1 (*Joint Controller Agreement*), the Authority shall be entitled to terminate this Contract by issuing a Termination Notice to the Supplier in accordance with Clause 39 (*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:

9.1.1 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 Contract, and provide evidence of such due diligence to the other Party where reasonably requested; and

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

10. Data Retention

10.1 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 their privacy 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 Contract), and taking all further actions as may be necessary to ensure its compliance with Data Protection Legislation and its privacy policy.

Annex 2: International Data Transfer Agreement and International Data Transfer Agreement Addendum to the EU Commission Standard Contractual Clauses

Not Used

Annex 3: Standard Contractual Clauses for EU GDPR Compliant Transfers

Not Used