General Data Protection Regulation (GDPR)

Law : means any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Supplier is bound to comply;

Supplier Personnel : means all directors, officers, employees, agents, consultants. contractors and suppliers of the Supplier and/or of any Sub-processor engaged in the performance of its obligations under the Service Agreement(s)

General:

i. Each Party shall bear its own costs and expenses in relation to the preparation, negotiation and execution of this Amending Agreement.
ii. GOVERNING LAW AND JURISDICTION
    a. This Agreement and any claim or dispute arising out of it or its subject matter shall be governed by and interpreted in accordance with the laws of England.
    b. Each Party irrevocably submits to the exclusive jurisdiction of the English courts in relation to all matters arising out of or in connection with this Agreement.

DEFINITIONS:

Customer: identified as the recipient of services this Agreement listed in the Appendix A to this Agreement from time to time and includes any third party for whom the Supplier Processes Personal Data listed in the Schedule(s) to this Data Processing Agreement.
Data Protection Legislation :

(i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time

(ii) the DPA 2018 to the extent that it relates to processing of personal data and privacy;

(iii) all applicable Law about the processing of personal data and privacy;

Data Protection Impact Assessment : an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data.

Process, Controller, **Processor** , **Data Subject** , **Personal Data** , **Personal Data Breach** , **Data Protection Officer** take the meaning given in the GDPR.

Data Loss Event : any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Agreement, and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.

Data Subject Access Request : a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data.

DPA 2018 : Data Protection Act 2018

GDPR : the General Data Protection Regulation *(Regulation (EU) 2016/679)*

LED : Law Enforcement Directive *(Directive (EU) 2016/680)*

Protective Measures : appropriate technical and organisational measures taking into account the level of damage and/or distress that a Data Subject might suffer resulting from any accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted stored or otherwise processed, which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the such measures adopted by it.

Sub-processor : any third Party appointed to process Personal Data on behalf of the Supplier related to any of the Services Agreements listed in the Appendix to this Data Processing Agreement.

Service Agreement: an agreement between Customer and Supplier under which the Supplier Processes Personal Data on behalf of the Customer.

1. DATA PROTECTION

1.1 This Data Processing Agreement applies if and to the extent Supplier Processes Customer's Personal Data in the course of providing the services set out in a Service Agreement. Customer appoints Supplier as Processor for those purposes.

1.2 Where clause 1.1 does not apply but the Supplier Processes Personal Data

(a) limited to business contact details of the Customer's personnel (employees, agents and subcontractors);

(b) for purposes limited to its administration of a contract with the Customer which does not otherwise involve Processing of Personal Data;

it will do so as Controller strictly in accordance with Data Protection Legislation and Law.

1.3 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Supplier is the Processor of the Personal Data listed in a Schedule to this Data Processing Agreement, unless the Customer is processing Personal Data on behalf of a third party Client, in which case that third party Client is the data Controller. The only processing of such Data that the Supplier is authorised to do is listed in a Schedule to this Data Processing Agreement and may not be determined by the Supplier.

1.4 The Supplier shall notify the Customer immediately if it considers that any of the Customer's instructions infringe the Data Protection Legislation.

1.5 The Supplier shall provide all reasonable assistance to the Customer in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Customer and/or the Client, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Services;

(c) an assessment of the risks to the rights and freedoms of Data Subjects; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.

1.6 In relation to any Personal Data processed in connection with its obligations under the Services Agreement the Supplier shall:

(a) process that Personal Data only in accordance with the Schedule to this Data Processing Agreement, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Customer before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Customer 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;

(c) ensure that :

(i) the Supplier Personnel do not process Personal Data except in accordance with this Data Processing Agreement;

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Supplier's duties under this Data Processing Agreement;

(B) are subject to appropriate confidentiality undertakings with the Supplier or any Sub-processor;

(C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third Party unless directed in writing to do so by the Customer or as otherwise permitted by this Data Processing Agreement; and

(D) have undergone and regularly refresh adequate training in the use, care, protection and handling of Personal Data; and

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Customer and/or the Customer's Client has been obtained and the following conditions are fulfilled:

(i) the Customer or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Customer;

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

(iii) the Supplier 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 Customer in meeting its obligations); and

(iv) the Supplier complies with any instructions notified to it in advance by the Customer with respect to the processing of the Personal Data;

(e) on termination of a Services Agreement at the written direction of the Customer, delete or return the relevant Personal Data (and any copies of it together with any encryption keys or other means required to enable the Customer to Process the Personal Data) to the Customer or the Client unless the Supplier is required by Law to retain the Personal Data.

1.7 Subject to clause 1.8, the Supplier shall notify the Customer immediately if it:

(a) receives a Data Subject Access Request (or purported Data Subject Access Request);

(b) receives a request to rectify, block or erase any Personal Data;

(c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

(d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data processed under this Agreement

(e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or

(f) becomes aware of a Data Loss Event

in each case related to Personal Data Processed by it under this Data Processing Agreement.

1.8 The Supplier's obligation to notify under clause 1.7 shall include the provision of further information to the Customer in phases, as details become available and without the need for Customer to make a request.

1.9 Where the Supplier becomes aware of a Data Loss Event the notification under Clause 1.7 will at a minimum:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) describe the likely consequences of the personal data breach;

(c) describe the measures taken or proposed to be taken by the Supplier to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects. The Supplier shall take such measures without delay.

1.10 Taking into account the nature of the processing, the Supplier shall provide the Customer and the Client with full assistance in relation to either Party's obligations under Data Protection Legislation and in respect of any complaint, communication or request referred to in clause 1.9 (and insofar as possible within the timescales reasonably required by the

Customer to enable the Customer and/or the Client to comply with Data Protection Legislation) including by promptly providing:

(a) the Customer with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Customer to enable the Customer and/or the Client to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

(c) the Customer, at its request, with any Personal Data it holds in relation to a Data Subject;

(d) assistance as requested by the Customer and/or the Client following any Data Loss Event;

(e) assistance as requested by the Customer and/or the Client with respect to any request from the Information Commissioner's Office, or any consultation by the Customer with the Information Commissioner's Office.

1.11 The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Data Processing Agreement (including but not limited to the record of processing required by Article 30 GDPR). This requirement does not apply where the Supplier employs fewer than 250 staff, unless:

(a) the processing is not occasional;

(b) the processing includes special categories of data as referred to in Article 9 (1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; and

(c) the processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.12 The Supplier shall permit the Customer and/or the Client or the Customer's designated auditor to carry out periodic audits and/or inspections of its Data Processing activity, subject to appropriate confidentiality provisions, to reasonable notice and to the audit being carried out within normal working hours unless required as a matter of urgency, for example in connection with a Data Loss Event.

1.13 The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.14 Before allowing any Sub-processor to process any Personal Data related to this Agreement, the Supplier must:

(a) notify the Customer in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Customer and/or the Client;

(c) enter into a written agreement with the Sub-processor which give effect to the terms set out in this Data Processing Agreement such that they apply to the Sub-processor; and

(d) provide the Customer and/or the Client with such information regarding the Sub-processor as the Customer may reasonably require and afford the Customer an opportunity to object.

1.15 The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.

1.16 The liability of each party to the other in respect of or arising out of damages incurred by a Data Subject as a result of a breach of Data Protection Legislation shall be governed by the Data Protection Legislation. The liability of the parties to each other for all other breaches of this Amending Agreement shall be limited by the relevant provision(s) of the relevant Services Agreement as amended by this Amending Agreement.

1.17 The Customer and /or the Client may, at any time on not less than 30 Working Days' notice, revise this Data Processing Agreement (including the Schedule) by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement), or if required to reflect the terms of any Agreement under which the Customer performs Processing of Personal Data for a third party Client as Controller.

1.18 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Customer and/or the Client may on not less than 30 Working Days' notice to the Supplier require this Data Processing Agreement to be amended to ensure that it complies with any guidance issued by the Information Commissioner's Office.

1.19 The Parties shall agree the Supplier's reasonable charges arising out of or in connection with any change to the Services required to comply with Data Protection Legislation.

Annexure to Appendix B

NOTE – Where the Customer Processes Personal Data (limited to business contact details) of the Supplier's personnel (employees, agents and subcontractors) as Controller for the purposes of contract administration it will do so strictly in accordance with Data Protection Legislation.

The Schedule below will not apply unless and until Customer's Processing of Personal Data for Supplier falls outside the above purpose. At that time the Parties must complete the required information.

For the purposes of the Data Processing Agreement the parties have designated the following Data Protection Officers or other contacts. The parties will keep these details up to date.

DATA PROTECTION OFFICERS

Supplier	**NAME** Peter Cashmore NHS Shared Business Services Limited **EMAIL** Legal.services@soprasteria.com
Customer	**NAME** *(name of DPO or responsible contact)* **EMAIL**

Schedule to Annexure B - Processing, Personal Data and Data Subjects

Description	Details
Subject matter of the processing	*For the purpose of providing access to NHS SBS Framework agreement(s)*
Duration of the processing	*Duration of your contract with NHS Shared Business Services.*
Nature and purposes of the processing	*NHS SBS may undertake processing of personal data as part of the provision of following Procurement services:* • *Associate Member Access to Framework Agreements*
Type of Personal Data	Name, address, telephone number of patient (See Instructions)
Categories of Data Subject	NHS SBS Staff, Associate Member, Suppliers
Plan for return and destruction of the data once the processing is complete UNLESS requirement under union or member state law to preserve that type of data	The data will be retained in line with the NHS Records Management Code of Practice. *Customer to cover the costs for any onward retention or destruction of data as required post the retention period for the lifecycle of the data.*

INSTRUCTIONS

The Supplier shall comply with the Services Contract and any further written instructions of the Customer with respect to processing of Customer Data.

Any such further instructions shall be incorporated into or referenced in this Schedule.

Instructions	• Associate Members should refer to the Guidelines given by Crown Commercial Services Procurement Policy Note 03/17 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/674575/FINAL_PUBLISHED_GDPR_PPN_03-17.docx.pdf • On a Purchase Order, the Associate Member should ensure that any use or transfer of personal identifiable data does not contravene GDPR Regulations