

Work Order

This document is a Work Order according to the definitions contained within the provisions of the Services Delivery Agreement (SDA) dated **18th February 2020**, between **Bloom Procurement Services Ltd** and **Ernst & Young LLP**.

Except where stated herein, all the clauses and conditions specified in the said supplier terms are included herein by reference and form part of this Work Order.

For the avoidance of doubt, the Bloom Standard Terms & Conditions (only where applicable), the SDA and this Work Order constitute the contract between Bloom and the SPS Provider and are hereinafter referred to collectively as the Supplier Terms.

We are delighted to advise that **Bloom Procurement Services Ltd** have been authorised to obtain the following services on behalf of the Authority.

Project Number:	Project_6863 Contract_16184
Project Name:	NEPRO3 - InSite Programme - Data Transformation
SPS Provider:	Ernst & Young LLP
For the Attention of:	REDACTED TEXT under FOIA Section 40, Personal Information
E-mail:	REDACTED TEXT under FOIA Section 40, Personal Information
Telephone Number:	REDACTED TEXT under FOIA Section 40, Personal Information
Address:	REDACTED TEXT under FOIA Section 40, Personal Information

Description of Specialist Professional Services / deliverables required:

Ernst & Young LLP (EY) have been appointed by Bloom Procurement Services Limited on behalf of Cabinet Office (CO) to -

- Develop the data programme management plan to seed a self-perpetuating data led culture in the estates and property functions across departments.
- Build a data maturity framework that will enable maturity initiatives to land at a progressive pace within each department using industry standard measures line Organisational Management Maturity Model (OM3).

A key design principle of the operating model is the ability to implement solutions with a restricted level of direct intervention or resources from the centre into departmental efforts. Therefore, all outputs need to be designed keeping this principle in mind.

Detailed Requirements

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

--

Milestones REDACTED TEXT under FOIA Section 43 (2), Commercial Information
Service Levels and Key Performance Indicators (KPIs) REDACTED TEXT under FOIA Section 43 (2), Commercial Information
Contract Management (Measuring Success and Review) REDACTED TEXT under FOIA Section 43 (2), Commercial Information



--

Any Further Specific Requirements	REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Invoicing procedure

The SPS Provider shall complete and submit a Payment Request/Highlight Report via the Technology Platform. This will initiate the Self-Billing Process once approved by the Authority or requirement owner.

Milestone reporting and Payment (Subject to agreed Payment Request/Highlight Report) Payment Schedule

Description	Deliverables	Planned Payment Request Submission Date	Total Price
1.1	REDACTED TEXT under FOIA Section 43 (2), Commercial Information	REDACTED TEXT under FOIA Section 43 (2), Commercial Information	REDACTED TEXT under FOIA Section 43 (2), Commercial Information
Total:			£100,000.00

Total Price	Commencement Date	Currency
£100,000.00	11 th February 2025	Pounds Sterling

Acknowledgment re supervision and control of SPS Provider personnel.

By signing this Work Order and agreeing to the Supplier Terms, the SPS Provider confirms for the duration of the Services provided (subject to the contractual terms governing the Services to be provided):

1. The SPS Provider shall procure that its personnel do not act or operate in a manner which could be perceived in such a way as to infer that the SPS Provider's personnel are employees of the Authority;
2. The SPS Provider shall always ensure that the Authority shall not supervise or control the work being carried out by the SPS Provider's personnel;
3. The SPS Provider is free to determine the personnel it uses to provide the services provided that all personnel meet the standards specified by the Authority (including security clearances where applicable);
4. The SPS Provider shall not assume any line management responsibility for any of the Authority's employees;
5. The SPS Provider shall use their own equipment to deliver the Services, except where the provision of equipment by the Authority is necessary for security purposes;
6. The SPS Provider shall determine their own place and hours of work, except where the nature of the project naturally enforces restriction e.g. attending project meetings at client site during business hours;

If at any time, the SPS Provider fails to comply with the above terms, this shall amount to a material breach of the Work Order which is not capable of remedy for the purposes of the termination clause of the SDA and

this Work Order will be terminated with immediate effect. If the SPS Provider breaches these provisions it may be liable for the payment of income tax or national insurance contributions.

ANNEX 1 – to record permitted project specific processing of personal data.

1. The Contractor shall comply with any further written instructions with respect to processing by the Data Controller.
2. Any such further instructions shall be incorporated into this Schedule and this Schedule may be amended at any time during the Term by agreement in writing between the Data Controller and the Contractor to ensure that the description and detail set out in this Schedule with regard to the processing of personal data reflects the arrangements between the Parties, is accurate and is compliant against the Data Protection Legislation.

No	Description	Details
1	Subject Matter of the Processing	The processing of personal data in relation to the obligations of the SPS Provider as the supplier under the contract for Specialist Professional Services
2	Duration of the Processing	The data will be provided for the duration of the Project covering for the provision of specialist professional services. The contract expires on the project end date at which time the information will be reviewed.
3	Nature and Purposes of the Processing	The nature of the processing includes the collection, recording, organisation storage, retrieval, use, disclosure by transmission, dissemination or otherwise making available, erasure or destruction of data (whether by automated means) The purpose of the processing is the fulfillment of the SPS Providers obligations arising under the Work Order for the provision of specialist professional services and to ensure effective communication between the SPS Provider and the Authority.
4	Type of Personal Data	For the purposes of the contract, the Authority will disclose the following information directly to the SPS Provider: <ul style="list-style-type: none"> - Contact details for individuals concerned with the management of the Work Order - Contact details for individuals concerned with specific projects under the Work Order - (Name, email address, postal address, telephone number)
5	Categories of Data Subject	Personal data relating to the Authorities staff (including temporary or agency staff) concerned with the Work Order (Name, email address, postal address, telephone number)
6	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 SPS Provider agrees that all data supplied will be retained no longer that is necessary after the expiry or termination of the Work Order and shall be destroyed as soon as practicable. All estates and property data and information from internal meetings and governance boards shall be treated as commercially sensitive and cannot be used outside of the provision of the services within this contract

ANNEX 2

1. This Annex lists the sub-processors that the Data Controller has authorised the Contractor to use in accordance with the Supplier Terms.
2. The Data Controller may, at any time and upon such notice as is reasonable in the circumstances, withdraw its approval in relation to any or all sub-processors listed within this Annex and upon such withdrawal the Contractor must immediately cease using that sub-processor.
3. If the Contractor wishes to propose a new sub-processor for approval, it must provide written notice to the Data Controller detailing the identity of the proposed sub-processor, the nature of the sub-processing and confirmation that a written contract in relation to the sub-processing is in place between the Contractor and the sub-processor. The Data Controller must not unreasonably refuse or delay approval.
4. The Data Controller may at any time and upon reasonable notice request copies of the contracts between the Contractor and its approved sub –processors in relation to the sub-processing.

Sub-contractor details: (name, address and company registration number)	Nature of sub-processing:	Commencement date and term of contract between Contractor and Sub-processor:
N/A	N/A	N/A

Signature Area

Annex 3 - Cabinet Office Information Security Management Requirements

Information Security Management Cabinet
Office project requirements for
Consultancy/Professional Services

Cabinet Office Options

Risk assessment

The Cabinet Office has assessed this Agreement as	a standard consultancy agreement	<input checked="" type="checkbox"/>
	a higher-risk consultancy agreement	<input type="checkbox"/>

Relevant Certifications

Where the Cabinet Office has assessed this Agreement as a standard consultancy agreement, it requires the SPS Provider to be certified as compliant with:	Cyber Essentials	<input checked="" type="checkbox"/>
	Cyber Essentials Plus	<input type="checkbox"/>

SPS Provider obligations

Where the Cabinet Office has assessed this Agreement as a higher-risk consultancy agreement, the SPS Provider must comply with all requirements in this Schedule Annex 1 (Security Management).

Where the Cabinet Office has assessed this Agreement as a standard consultancy agreement, the SPS Provider must comply with this Schedule Annex 1 (Security Management), other than: the requirement to be certified as compliant with ISO/IEC 27001:2013 under Paragraph 0;

the requirement to undertake security testing of the SPS Provider Information Management System in accordance with paragraph 3 of Appendix 1; the requirement to produce a Security Management Plan in accordance with Paragraph 0

the requirement to document unencrypted Cabinet Office Data in the Security Management Plan in accordance with paragraph 5.4 of Appendix 1

Definitions

In this Schedule Annex 1 (Security Management):

“Anti-virus Software”	<p>means software that:</p> <ul style="list-style-type: none"> protects the SPS Provider Information Management System from the possible introduction of Malicious Software; scans for and identifies possible Malicious Software in the SPS Provider Information Management System; if Malicious Software is detected in the SPS Provider Information Management System, so far as possible: <ul style="list-style-type: none"> prevents the harmful effects of the Malicious Software; and removes the Malicious Software from the SPS Provider Information Management System.
------------------------------	---

“Breach of Security”	<p>means the occurrence of:</p> <p>any unauthorised access to or use of the Services, the Cabinet Office Premises, the Sites, the SPS Provider Information Management System and/or any information or data used by the Cabinet Office, the SPS Provider or any Sub-contractor in connection with this Agreement;</p>
	<p>the loss (physical or otherwise) and/or unauthorised disclosure of any information or data, including copies of such information or data, used by the Cabinet Office, the SPS Provider or any Subcontractor in connection with this Agreement; and/or</p> <p>any part of the SPS Provider Information Management System ceasing to be compliant with the Certification Requirements.</p>
“Cabinet Office Data”	<p>means any:</p> <p>data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic, magnetic, optical or tangible media; or</p> <p>Personal Data for which the Cabinet Office is a, or the, Data Controller,</p> <p>that is:</p> <p>supplied to the SPS Provider by or on behalf of the Cabinet Office; or</p> <p>that the SPS Provider generates, processes, stores or transmits under this Agreement.</p>
“Cabinet Office Equipment”	<p>means any hardware, computer or telecoms devices, and equipment that forms part of the Cabinet Office System.</p>
“Cabinet Office System”	<p>means the information and communications technology system used by the Cabinet Office to interface with the SPS Provider Information Management System or through which the Cabinet Office receives the Services.</p>
“Certification Default”	<p>means the occurrence of one or more of the circumstances listed in paragraph 0.</p>
“Certification Rectification Plan”	<p>means the plan referred to in paragraph 0.</p>
“Certification Requirements”	<p>means the information security requirements set out in paragraph 0.</p>
“Cyber Essentials”	<p>means the Cyber Essentials certificate issued under the Cyber Essentials Scheme.</p>

“Cyber Essentials Plus”	means the Cyber Essentials Plus certificate issued under the Cyber Essentials Scheme.
“Cyber Essentials Scheme”	means the Cyber Essentials scheme operated by the National Cyber Security Centre.
“End-user Device”	means any personal computers, laptops, tablets, terminals, smartphones or other portable electronic device used in the provision of the Services.
“HMG Baseline Personnel Security Standard”	means the employment controls applied to any individual member of the SPS Provider Personnel that performs any activity relating to the provision or management of the Services, as set out in “HMG Baseline Personnel Standard”, Version 6.0, May 2018 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/714002/H

	MG_Baseline_Personnel_Security_Standard_-_May_2018.pdf), as that document is updated from time to time.
“Malicious Software”	means any software program or code intended to destroy, interfere with, corrupt, remove, transmit or cause undesired effects on program files, data or other information, executable code, applications, macros or configurations.
“NCSC Cloud Security Principles”	means the National Cyber Security Centre’s document “Implementing the Cloud Security Principles” as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/cloudsecurity/implementing-the-cloud-security-principles .
“NCSC Device Guidance”	means the National Cyber Security Centre’s document “Device Security Guidance”, as updated or replaced from time to time and found at https://www.ncsc.gov.uk/collection/device-security-guidance .
“Privileged User”	means a user with system administration access to the SPS Provider Information Management System, or substantially similar access privileges.
“Process”	means any operation performed on data, whether or not by automated means, including 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 that data.
“Prohibited Activity”	means the storage, access or Processing of Cabinet Office Data prohibited by a Prohibition Notice.
“Prohibition Notice”	means a notice issued under paragraph 1.3 of Appendix 1.
“Relevant Certifications”	means those certifications specified in paragraph 0.

“Relevant Convictions”	means any previous or pending prosecution, conviction or caution (excluding any spent conviction under the Rehabilitation of Offenders Act 1974) relating to offences involving dishonesty, terrorism, immigration, firearms, fraud, forgery, tax evasion, offences against people (including sexual offences), or any other offences relevant to Services as the Cabinet Office may specify.
“Security Management Plan”	means the document prepared in accordance with the requirements of paragraph 0.
“Sites”	<p>means any premises: from or at which: the Services are (or are to be) provided; or the SPS Provider manages, organises or otherwise</p> <p style="padding-left: 100px;">directs the provision or the use of the Services; or</p> <p>where:</p> <p style="padding-left: 100px;">any part of the SPS Provider Information Management System is situated; or</p> <p style="padding-left: 100px;">any physical interface with the Cabinet Office System takes place.</p>
“Standard Contractual Clauses”	means the standard data protection clauses specified in Article 46 of the United Kingdom General Data Protection Regulation setting out the appropriate safeguards for the transmission of personal data outside the combined territories of the United Kingdom and the European Economic Area.
“SPS Provider Information Management System”	<p>means:</p> <p style="padding-left: 40px;">those parts of the information and communications technology system and the Sites that the SPS Provider or its Sub-contractors will use to provide the Services; and</p> <p style="padding-left: 40px;">the associated information assets and systems (including organisational structure, controls, policies, practices, procedures, processes and resources);</p>
“Sub-contractor Personnel”	<p>means:</p> <p style="padding-left: 40px;">any individual engaged, directly or indirectly, or employed, by any Sub-contractor; and</p> <p style="padding-left: 40px;">engaged in or likely to be engaged in:</p> <p style="padding-left: 80px;">the performance or management of the Services; or</p> <p style="padding-left: 80px;">the provision of facilities or services that are necessary for the provision of the Services.</p>
“SPS Provider Personnel”	means any individual engaged, directly or indirectly, or employed by the SPS Provider or any Sub-contractor in the management or performance of the SPS Provider’s obligations under this Agreement.

“UKAS”	means the United Kingdom Accreditation Service.
--------	---

Introduction

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Principles of security

. REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Access to SPS Provider Personnel and SPS Provider Information Management System

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Certification Requirements

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Security Management Plan

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

REDACTED TEXT under FOIA Section 43 (2), Commercial Information



Notices

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

REDACTED TEXT under FOIA Section 43 (2), Commercial Information

Signature Area

Organisation Name:

**REDACTED TEXT under
FOIA Section 40, Personal
Information**

Role/Title:

**REDACTED TEXT under
FOIA Section 40, Personal
Information**

Name:

**REDACTED TEXT under
FOIA Section 40, Personal
Information**

Signature: **REDACTED TEXT
under FOIA Section 40,
Personal Information**

Organisation Name:

**REDACTED TEXT under
FOIA Section 40, Personal
Information**

Role/Title: **REDACTED TEXT
under FOIA Section 40,
Personal Information**

Name:

**REDACTED TEXT under
FOIA Section 40, Personal
Information**

Signature: **REDACTED TEXT
under FOIA Section 40,
Personal Information**