Appendix A

**Statement of Work**

1. **DURATION**

The Services shall commence on **22nd April 2025.** This SOW will expire, unless terminated earlier in accordance with the Agreement, on **28th May 2025**. The agreement is for a **total of 5 weeks.**

1. **SERVICES AND DELIVERABLES**

**Context**

DS Smith currently manages compliance responsibilities and associated documents through fragmented and inconsistent SharePoint-based processes. This lack of centralisation limits operational efficiency, data governance, and control across its sites. A unified, secure, and scalable platform is required to streamline compliance tracking and documentation management across all sites.

**Requirements**

DS Smith requires a web-based compliance tracker integrated with a document repository.

The system must:

* Enable secure uploads and management of Word, PDF, and Excel files
* Provide Single Sign-On (SSO) integration and role-based access control
* Ensure each user accesses only site-relevant data
* Maintain document retention policies (minimum of 2 years)
* Support sub-8 second document uploads

**Proposal**

Exponentia.ai proposes to deliver a centralized Compliance Data Management Tool tailored to DS Smith’s needs. The solution will combine compliance tracking and document repository features into a single platform, improving data security and operational workflows. A dedicated team (Project Manager, Architect, Developer, and DevOps) will ensure timely delivery and successful deployment of the system hosted on DS Smith's AWS infrastructure.

**Scope of Work**

Web Form Module

* A standardized form interface for site users to enter compliance responsibilities
* Validation rules to ensure data quality and consistency

Document Upload Module

* UI to upload and retrieve documents from a central repository
* Support for standard file types (Word, Excel, PDF)

Storage and Integration Layer

* Integration of UI with a backend storage solution for structured (form data) and unstructured (documents) data
* Use of Amazon DynamoDB and S3 for storage

Security and Access Control

* Role-based access control enforcing site-specific permissions

**High Level Plan**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Stage** | **Activity** | **W1** | **W2** | **W3** | **W4** | **W5** |
| Planning & Design | Wireframing and Planning |  |  |  |  |  |
| Planning & Design | Solution Architecture |  |  |  |  |  |
| Build | UI Development |  |  |  |  |  |
| Build | Backend Integration |  |  |  |  |  |
| Testing | Testing and Rollout |  |  |  |  |  |

1. **DELIVERABLES AND ACCEPTANCE CRITERIA**

|  |  |  |
| --- | --- | --- |
|  | **Work Product Description** | **Outcomes** |
| WP 1 |  |  |
| WP 2 |  |  |
| WP 3 |  |  |
| WP 4 |  |  |

1. **PROJECT MONITORING AND GOVERNANCE**
   1. The DS Smith IT Lead will be responsible for the day-to-day progress and output quality.
   2. In the event when the team is unable to meet the deliverables, the DS Smith IT Lead shall provide to a reasonable explanation and the revised completion schedule.
   3. The resources will adhere to the standard project management practice set by DS Smith.
   4. The key stakeholders from DS Smith are as follows:

|  |  |
| --- | --- |
| **Name** | **Designation/Role** |
| Wychard Draaijer | Group Property Project Manager |
| Sanjay Kumar | Head of Exponentia.ai UK |
| Jonathan Jones | Head of Facilities Management |
| Matthew Travis | Group Facilities Manager |

1. **CHARGES AND PAYMENT SCHEDULE**

Team structure and commercials for 5 weeks is given below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Role** | **Experience** | **Location** | **Total Days** | **Cost** |
| Squad Lead/ BA | 5-8 Years | India | 25 | £5,580 |
| Solution Architect | 8+ Years | India | 10 | £4,250 |
| DevOps Engineer | 5-8 Years | India | 5 | £1,255 |
| Python Developer | 5-8 Years | India | 20 | £5,580 |
| Tester | 3-5 Years | India | 5 | £1,035 |
| **Total Cost for the 5 week engagement** | | | | **£20,295 + VAT** |

**\* A month is assumed to have 20 days**

The above commercials exclude travel costs. The provider understands that this resource will work from an offshore location and there will be no requirement for the resource to travel to DS Smith offices in the UK. If there is a need for travel to the DS Smith office in the UK, DS Smith will cover the expenses for accommodation, travel, and per diem.

The payment milestone is as follows:

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Milestone** | **Charges (£)** |
| 1. | 100% Advaned Payment | £20,295 +VAT |

1. **ASSUMPTIONS, RISKS AND DEPENDENCIES**

**Assumptions and Dependencies**

* DS Smith will provide finalized input fields (e.g., Name, Email, Org) and a role matrix for user access setup across all site s.
* SSO will be supported through DS Smith’s existing authentication system (e.g., AD)
* Metadata standards (e.g., file naming conventions, file types) will be provided before development begins.
* The solution is expected to support standard compliance workloads — document volumes, file sizes, and concurrent users to be confirmed during discovery.
* Only standard file formats (PDF, Word, Excel) will be supported for upload and retrieval in this phase.
* No complex workflows, escalations, or multi-step automation are included in this MVP unless explicitly discussed.
* The compliance tracker and document repository will be deployed on DS Smith’s AWS, aligned with internal IT and security policies.

**Dependencies**

* DS Smith will provide access to existing systems, including SharePoint (if legacy document migration is required), and identity management systems for integration
* and testing.
* Timely provision of SSO configuration details, and access to AWS services or cloud environment provisioning support for setup and deployment.
* DS Smith will share a finalized user role matrix and access permissions across sites prior to role -based access implementation.
* All DS Smith locations will ensure sufficient network bandwidth and configurations to support sub -8 second document uploads and platform access.
* Key stakeholders and internal SMEs (e.g., IT Security, Data Governance) will be available for requirement validation, design reviews, and feedback throughout the
* project.
* DS Smith will provide all applicable compliance guidelines (e.g., GDPR, retention policies) prior to development kickoff
* DS Smith will allocate users, environments, and credentials for UAT, with at least a 1 -week buffer before testing begins, and provide timely feedback.

1. **CONSULTANTS**

Name of Consultants assigned: TBC

Role Titles: Squad Lead / BA, Solution Architect, DevOps Engineer, Python Developer and Tester.

1. **LOCATION**

The assignment will be delivered remotely.

1. **SUBCONTRACTORS**

In the event the Provider utilise the services of its approved Sub Contractors, the Provider will first communicate the name of its Sub Contractor to DS Smith and then it will ensure that such Sub Contractor(s) adhere to all the terms of this Appendix A and Agreement.

1. **ADDITIONAL TERMS**

I hereby acknowledge receipt and accept the contents of this Statement of Work.

For and on behalf of

**DS Smith**

Signed ................................................................

Name ..................................................................

Date ....................................................................

For and on behalf of

**[Exponentia AI Ltd.]**

Signed ................................................................

Name: Sanjay Kumar

(Head of Exponentia.ai UK)

Date:

Appendix C

**GDPR**

“**Data Protection Legislation**” means the Data Protection Act 1998 (“DPA”), EU Data Protection Directive 95/46/EC and EU Directive 2002/58/EC, in each case, as amended, revised or replaced from time to time (in particular, by operation of the Directive 2009/136/EC, and the General Data Protection Regulation (EU) 2016/679 (“GDPR”)) and all applicable national implementing legislation and guidelines, and any applicable analogous legislation in any jurisdiction, in each case, as amended, revised or replaced from time to time

# DATA PROTECTION

## In relation to the parties’ rights and obligations under this Agreement, the parties agree that the Customer is the “data controller” and Service Provider is the “data processor” as defined in the Data Protection Legislation. All terms used in this clause 6 that are defined in the Data Protection Legislation shall have the meaning given to them in the Data Protection Legislation.

## For the purposes of this Agreement, “**Customer Data**” shall mean the personal data or any part thereof of which the Customer is the data controller and which is processed by Service Provider on behalf of the Customer pursuant to this Agreement.

## The parties further agree that Customer Data:

### relates to data subjects who are former and current employees of the Customer;

### comprises personal identification and address details; communication means and contact details; education and training details; employment-related details; family, lifestyle and social circumstances; of such data subjects; and

### shall be processed by Service Provider in order to supply [the Services] and only for the duration of this Agreement or for such further time as the parties shall both agree in writing.

## Service Provider shall:

### carry out processing only in accordance with the Customer’s written instructions from time to time, including as set out in this Agreement, unless required to do otherwise by law in which case, where legally permitted, Service Provider shall inform the Customer of such legal requirement before processing;

### process the Customer Data only to the extent, and in such manner , as is necessary for the provision of the Services. The Service Provider may only correct, delete or block the Customer Data processing on behalf of the Customer as and when instructed to do so by the Customer;

### ensure that any Service Provider personnel authorised to process the Customer Data shall be subject to a binding duty of confidentiality in respect of such data and comply with the obligations in this Clause [1];

### take reasonable steps to ensure the reliability and competence of any Service Provider personnel who have access to the Customer Data;

### implement appropriate technical and organisational measures to protect the Customer Data against unauthorised or unlawful processing and accidental destruction, damage or loss, including the measures taken in accordance with applicable Data Protection Legislation, so as to allow the Customer to comply with its obligations under the Data Protection Legislation. At a minimum, these should include the requirements set out in Schedule [1] .The Service Provider shall provide a written description of the technical and organisational methods employed by the Service Provider for processing personal data (within the timescales required by the Customer);

### not subcontract any processing of the Customer Data without the Customer’s prior written consent. Such consent shall only be given where obligations in relation to the processing of the Customer Data that are the same as those imposed on Service Provider under this Agreement are imposed by contract on the subprocessor. The Service Provider shall remain fully liable to the Customer for any processing of the Customer Data conducted by a subprocessor appointed by Service Provider in accordance with this clause [ 1.4.6];

### at no additional cost, provide such information and such assistance to the Customer as the Customer may reasonably require, and within the timescales reasonably specified by the Customer, to allow the Customer to comply with its obligations under the Data Protection Legislation, including assisting the Customer to:

#### Comply with its own security obligations;

#### Discharge its obligations to respond to requests for exercising data subjects’ rights;

#### Comply with its obligations to inform data subjects about serious personal data breaches;

#### Carry out privacy impact assessments and audit privacy impact assessment compliance; and

#### Consult with the applicable supervisory authority following a privacy impact assessment;

### on expiry or termination of this Agreement, at the choice of the Customer, either promptly and securely return the Customer Data to the Customer or (unless its continued storage by Service Provider is required by law) promptly and securely delete the Customer Data;

### at no additional cost, keep or cause to be kept such information as is necessary to demonstrate compliance with its obligations under this clause[1], including full and accurate records relating to the processing of the Customer Data and shall, upon reasonable notice, make available to the Customer or grant to the Customer and its auditors and agents, and any applicable law enforcement authority (including any applicable supervisory authority), a right of access to, and to take copies of, any information or records kept by Service Provider pursuant to this clause [ ];

### inform the Customer immediately if, in Service Provider’s opinion, any instruction issued by the Customer pursuant to this clause [ ] breaches any provision of the Data Protection Legislation; and

### not transfer any of the Customer Data outside of the European Economic Area without the Customer's prior written consent.

## Service Provider shall notify the Customer without undue delay after becoming aware of any accidental, unauthorised or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to the Customer Data. Service Provider shall take such steps as the Customer, or any applicable law enforcement authority (including any applicable supervisory authority) may reasonably require, within the timescales reasonably required by such entities, to remedy such breach and provide such further information as any of those entities may reasonably require.

## Service Provider shall notify the Customer without undue delay in writing if it receives from any data subject whose personal data forms part of the Customer Data, or any applicable law enforcement authority (including any applicable supervisory authority):

### any communication seeking to exercise rights conferred on the data subject by the Data Protection Legislation;

### any complaint or any claim for compensation arising from or relating to the processing of the Customer Data; or

### any communication from any applicable law enforcement authority (including any applicable supervisory authority).

## Service Provider shall notify the Customer without undue delay in writing of any actual or suspected breach of this clause [1], and provide full and prompt information and assistance to the Customer and any applicable law enforcement authority (including any applicable supervisory authority) in relation to such breach at its cost. For the avoidance of doubt, a breach of this clause[1 ] does not constitute indirect or consequential loss for the purposes of clause[ ].

## If the European Commission lays down, or an applicable supervisory authority adopts, standard contractual clauses for the matters referred to in Article 28(3) and Article 28(4) of the General Data Protection Regulation pursuant to Article 28(7) or Article 28(8) of the General Data Protection Regulation (as appropriate) and Customer notifies Service Provider that it wishes to incorporate any element of any such standard contractual clauses into this Agreement, the Service Provider shall agree to changes as required by Customer in order to incorporate such elements in writing.

## Service Provider shall comply at all times with, and assist the Customer and any Customer affiliate in complying with its applicable obligations under, the Data Protection Legislation. Service Provider must not perform its obligations under this Agreement in such a way so as to cause the Customer and any Customer affiliate to breach any of its applicable obligations under the Data Protection Legislation.

## Service Provider shall indemnify, and keep indemnified, the Customer for all losses, damage, costs, fines or expenses (including legal expenses) incurred or suffered by the Customer relating to any failure by Service Provider to comply with its obligations in this clause [ ] and/or any breach by Service Provider of the Data Protection Legislation or any other applicable data protection legislation and/or any act or omission of Service Provider in relation to the Customer Data which puts the Customer in breach of its obligations under the Data Protection Legislation or any other applicable data protection legislation or in breach of its obligations to any regulatory body or under any other applicable law or regulation.

## The Customer shall own all rights, title and interest in and to all Customer Data. Service Provider hereby completely and irrevocably assigns to the Customer by way of present assignment of future rights all copyright, database rights, intellectual property rights and other rights of whatever nature in and to the Customer Data to the extent that they have been or are acquired by Service Provider. Service Provider shall execute and transfer any and all of the documents reasonably considered by the Customer to be necessary to ensure that the ownership of the Customer Data and all rights therein are vested in the Customer.