ORDER FORM – Lot 1 Integrated Service Providers

National LGPS Framework for Integrated Service Providers (ISP) and the Provision of Member Data Services
Reference number – NCCT42646

FROM

Customer	NHS Business Services Authority
Service Address	Stella House, Goldcrest Way, Newcastle upon Tyne, Tyne and Wear, NE15 8NY
Invoice Address	Stella House, Goldcrest Way, Newcastle upon Tyne, Tyne and Wear, NE15 8NY
Contact Ref:	W61784
Order Number	To be confirmed upon contract signature
Order Date	07/03/2025

TO

Provider:	Heywood Limited trading as Heywood Pension Technologies
For the attention of: E-mail Telephone number	[redacted] [redacted] [redacted]
Address	2nd Floor, 3 Barrington Road, Altrincham, WA14 1GY

1. TERM AND TERMINATION
Call-Off Commencement Date: As per contract signature date.
Initial Period: 3 years from the Service Commencement Date [redacted]
Notice Period for Extensions: N/A
Required Go-Live Date: 31st October 2025, or as otherwise amended in the DWP's Staged Timetable Connection

2. SERVICES
NHSBSA are looking to secure a contract for Heywood to be NHSBSAs Integrated Service Provider for Pension Dashboards. [redacted]

3. DELIVERABLES
[redacted]

[redacted]

4. CHARGES

[redacted]

[redacted]

5. SOLUTION TYPE

The solution is a software as a service (SAAS) solution. [redacted]

Enhancement Implementation Period: 12 months.

6. CUSTOMER SYSTEM
NHSBSA currently utilise Compendia 6.8 (in the process of being upgraded to Touch admin) and will provide regular extracts, as outlined in the file specification, that will be loaded via SFTP into the ISP Solution.

7. NOT USED
N/A

8. WARRANTY PERIOD
The Warranty Period shall be as defined in the Call-Off Terms and Conditions.

9. LIABILITY
[redacted]
[redacted]

10. REPORTING & GOVERNANCE

[redacted]

11. MANDATORY POLICIES

Not Applicable

12. QUALITY STANDARDS

The quality standards are set out in the Schedules to the Call-Off Terms and Conditions.

13. INSURANCE REQUIREMENTS

Public Liability: as per clause 26 of the Call-Off Terms and Conditions.

Professional Indemnity: as per clause 26 of the Call-Off Terms and Conditions.

14. DATA PROTECTION

The Customer agrees to the Provider appointing the following sub-processors:

[redacted]

[redacted]

[redacted]

[redacted]

15. CONFIDENTIAL INFORMATION

The following information shall be deemed Commercially Sensitive Information or Confidential Information:

This Call-Off Contract and all information contained in the Provider's proposal.

Duration that the information shall be deemed Commercially Sensitive Information or Confidential Information: Indefinitely

16. ADDITIONAL REQUIREMENTS

[redacted]

The Data Processing Schedule appended to this Order Form shall govern and detail the data processing undertaken for the Services.

The Provider will fulfil its social value obligation by its volunteering with Ribble Valley.

BY SIGNING AND RETURNING THIS ORDER FORM THE PROVIDER AGREES to enter a legally binding contract with the Customer to provide to the Customer the Services specified in this Order Form (together with, where completed and applicable, the mini-competition order (additional requirements) set out in section 2 of this Order Form) incorporating the rights and obligations in the Call-Off Terms and Conditions set out in the Framework Agreement entered into by the Provider and the Authority on 21 April 2024

For and on behalf of the Provider:-

Name and Title	
Signature	
Date	

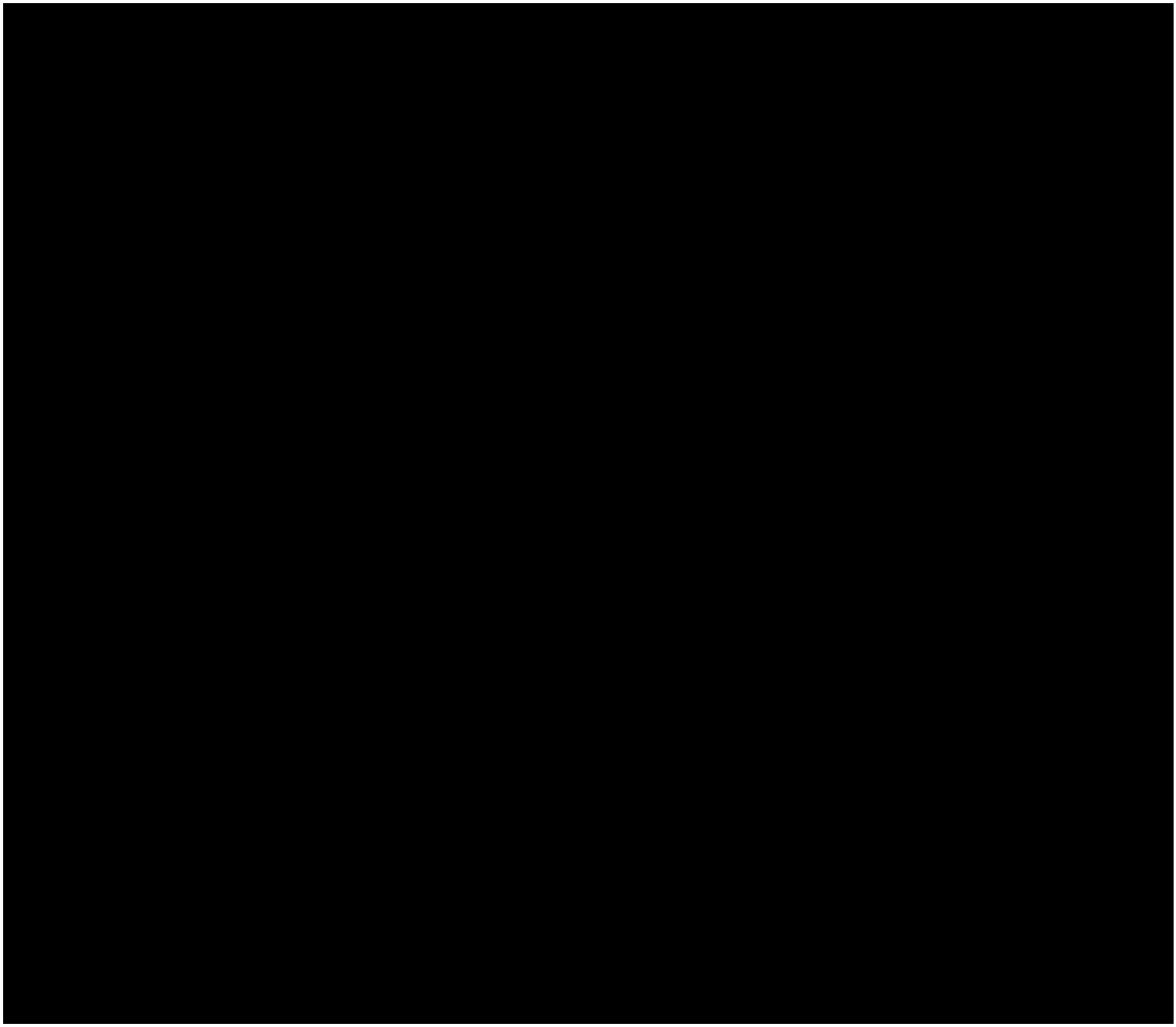
For and on behalf of the Customer:-

Name and Title	
Signature	
Date	

CALL-OFF SCHEDULE B

[redacted]

[redacted]



ORDER FORM PRODUCT SCHEDULE

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Security Schedule

[redacted]

Processing Data Schedule

1. **Status of the Controller**

1.1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA 2018. A Party may act as:

1.1.1. "Controller" in respect of the other Party who is "Processor";

1.1.2. "Processor" in respect of the other Party who is "Controller";

1.1.3. "Joint Controller" with the other Party;

1.1.4. "Independent Controller" of the Personal Data where the other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 *(*Processing Personal Data*)* which scenario they think shall apply in each situation.

2. **Where one Party is Controller and the other Party its Processor**

1.2. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 *(*Processing Personal Data) by the Controller and may not be determined by the Processor.

1.3. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

1.4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

1.4.1. a systematic description of the envisaged Processing and the purpose of the Processing;

1.4.2. an assessment of the necessity and proportionality of the Processing in relation to the Services;

1.4.3. an assessment of the risks to the rights and freedoms of Data Subjects; and

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

1.5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:

1.5.1. process that Personal Data only in accordance with Annex 1 *(*Processing Personal Data) unless the Processor is required to do otherwise by Law. If it is so required the Processor shall promptly notify the Controller before Processing the Personal Data unless prohibited by Law;

1.5.2. ensure that it has in place Protective Measures, including in the case of the Provider the measures set out in the Security Schedule*,* which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:

1.5.2.1. nature of the data to be protected;

1.5.2.2. harm that might result from a Data Loss Event;

1.5.2.3. state of technological development; and

1.5.2.4. cost of implementing any measures.

1.5.3. ensure that:

1.5.3.1. the Processor Personnel do not Process Personal Data except in accordance with this Contract (and in particular Annex 1 *(*Processing Personal Data));

1.5.3.2. it uses best endeavours to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:

1.5.3.2.1. are aware of and comply with the Processor's duties under this Schedule and the order form;

1.5.3.2.2. are subject to appropriate confidentiality undertakings with the Processor or any Subprocessor;

1.5.3.2.3. 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 Controller or as otherwise permitted by this Contract; and

1.5.3.2.4. have undergone adequate training in the use, care, protection and handling of Personal Data;

1.5.4. not transfer Personal Data outside of the UK; unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:

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

1.5.6. the Controller and/or the Processor have provided appropriate safeguards in relation to the transfer (whether in

accordance with UK GDPR Article 46 or section 75 of the DPA 2018) and/or Article 46 of the EU GDPR (where applicable) as determined by the Controller which could include relevant parties entering into:

1.5.7. where the transfer is subject to UK GDPR:

1.5.8. the International Data Transfer Agreement issued by the Information Commissioner under S119A(1) of the DPA 2018 (the "**IDTA**"); or

1.5.9. 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 ("**EU SCCs**") together with the UK International Data Transfer Agreement Addendum to the EU SCCs (the "**Addendum**"), as published by the Information Commissioner's Office from time to time under section 119A(1) of the DPA 2018; and/or

1.5.10. where the transfer is subject to EU GDPR, the EU SCCs,

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

1.5.12. the Data Subject has enforceable rights and effective legal remedies;

1.5.13. the Processor 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 Controller in meeting its obligations); and

1.5.14. the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data.

1.5.15. at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of this Contract unless the Processor is required by Law to retain the Personal Data.

1.6. Subject to Paragraph 2.6 of this Schedule, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with this Contract it:

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

1.6.2. receives a request to rectify, block or erase any Personal Data;

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

1.6.4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract;

1.6.5. 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

1.6.6. becomes aware of a Data Loss Event.

1.7. The Processor's obligation to notify under Paragraph 2.5 of this Schedule shall include the provision of further information to the Controller, as details become available.

1.8. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Paragraph 2.5 of this Schedule (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:

1.8.1. the Controller with full details and copies of the complaint, communication or request;

1.8.2. such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

1.8.3. the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;

1.8.4. assistance as requested by the Controller following any Data Loss Event; and/or

1.8.5. assistance as requested by the Controller with respect to any request from the Information Commissioner's Office or any other regulatory authority, or any consultation by the Controller with the Information Commissioner's Office or any other regulatory authority.

1.9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this This Schedule. This requirement does not apply where the Processor employs fewer than two hundred and fifty (250) staff, unless:

1.9.1. the Controller determines that the Processing is not occasional;

1.9.2. the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the UK GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the UK GDPR; or

1.9.3. the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.

1.10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.

1.11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.

1.12. Before allowing any Subprocessor to Process any Personal Data related to this Contract, the Processor must:

1.12.1. notify the Controller in writing of the intended Subprocessor and Processing;

1.12.2. obtain the written consent of the Controller;

1.12.3. enter into a written agreement with the Subprocessor which gives effect to the terms set out in this This Schedule such that they apply to the Subprocessor; and

1.12.4. provide the Controller with such information regarding the Subprocessor as the Controller may reasonably require.

1.13. The Processor shall remain fully liable for all acts or omissions of any of its Subprocessors.

1.14. The Parties agree to take account of any guidance issued by the Information Commissioner's Office or any other regulatory authority. The Customer may on not less than thirty (30) Working Days' notice to the Provider amend this Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office or any other regulatory authority.

3. Where the Parties are Joint Controllers of Personal Data

In the event that the Parties are Joint Controllers in respect of Personal Data under this Contract, the Parties shall implement Paragraphs that are necessary to comply with UK GDPR Article 26 based on the terms set out in Annex 2 (Joint Controller Agreement) to this This Schedule (Processing Data).

4. Independent Controllers of Personal Data

1.1. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.

1.2. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.

1.3. Where a Party has provided Personal Data to the other Party in accordance with Paragraph 4.2 of this This Schedule above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.

1.4. The Parties shall be responsible for their own compliance with Articles 13 and 14 UK GDPR in respect of the Processing of Personal Data for the purposes of this Contract.

1.5. The Parties shall only provide Personal Data to each other:

1.5.1. to the extent necessary to perform their respective obligations under this Contract;

1.5.2. in compliance with the Data Protection Legislation (including by ensuring all required fair processing information has been given to affected Data Subjects);

1.5.3. where the provision of Personal Data from one Party to another involves transfer of such data to outside the UK, if the prior written consent of the non-transferring Party has been obtained and the following conditions are fulfilled:

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

1.5.3.2. 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 determined by the non-transferring Party which could include:

1.5.3.2.1. where the transfer is subject to UK GDPR:

1.5.3.2.1.1. the 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

1.5.3.2.1.2. 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**") as published by the Information Commissioner's Office from time to time; and/or

1.5.3.2.2. 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;

1.5.3.3. the Data Subject has enforceable rights and effective legal remedies;

1.5.3.4. 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

1.5.3.5. 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

1.5.4. where it has recorded it in Annex 1 *(*Processing Personal Data*).*

1.6. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the UK GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the UK GDPR.

1.7. A Party Processing Personal Data for the purposes of this Contract shall maintain a record of its Processing activities in accordance with Article 30 UK GDPR and shall make the record available to the other Party upon reasonable request.

1.8. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the

Personal Data provided to it by the other Party pursuant to this Contract ("**Request Recipient**"):

1.8.1. the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or

1.8.2. where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:

1.8.2.1. promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and

1.8.2.2. provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.

1.9. Each Party shall promptly notify the other Party upon it becoming aware of any Data Loss Event relating to Personal Data provided by the other Party pursuant to this Contract and shall:

1.9.1. do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Data Loss Event;

1.9.2. implement any measures necessary to restore the security of any compromised Personal Data;

1.9.3. work with the other Party to make any required notifications to the Information Commissioner's Office or any other regulatory authority and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and

1.9.4. not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.

1.10. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under this Contract as specified in Annex 1 *(*Processing Personal Data*).*

1.11. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under this Contract which is specified in Annex 1 *(*Processing Personal Data).

1.12. Notwithstanding the general application of Paragraphs 2.1 to 2.14 of this Schedule to Personal Data, where the Provider is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with Paragraphs 4.2 to 4.12 of this Schedule.

Annex 1 - Processing Personal Data

1. This Annex 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 Annex shall be with the Customer at its absolute discretion.

   1.1 The contact details of the Customer's Data Protection Officer are: [redacted]

   1.2 The contact details of the Provider's Data Protection Officer are: [redacted]

   1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.

   1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	**The Customer is Controller and the Provider is Processor** The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Provider is the Processor of the following Personal Data: • Personal data that is shared under the Contract, for provision of NHSBSAs Integrated Service Provider for Pension Dashboards., information requested under data protection or freedom of information legislation, details of any personal data breaches, personal data used to monitor performance under the contract and handle complaints etc. **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* Provider Personnel for which the Provider is the Controller, • Personally identifiable information of any directors, officers, employees, agents, consultants and contractors of Customer (excluding the Provider Personnel) engaged in the performance of the Customer's duties under this Contract) for which the Customer is the Controller.

Description	Details
Subject matter of the Processing	The processing is needed in order to ensure that the Provider can effectively deliver the contract to provide services under the contract.
Duration of the Processing	The processing will continue for the duration of the Term of the Contract for an Initial Period: 3 years from the Service Commencement Date [redacted] and/or for such time as is considered necessary for the purposes of or in connection with the Provider's compliance with its obligations under this Contract which shall be stipulated by the Controller Also see "Plan for return and destruction of the data once the Processing is complete" below.
Nature and purposes of the Processing	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. As above, the processing is needed in order to ensure that the Provider can effectively deliver the contract to provide services under the contract. The Data processing is detailed in section 4 of the Order Form. The Customer will provide the Provider the information required by the Provider to enable the Provider to complete the contract which will include Personal Data. The Provider may store any Personal Data processed for the purposes of completing the Services as agreed between the parties in accordance with this Annex 1.
Type of Personal Data being Processed	First Name, Last name, previous last name, date of birth, NI number, current postal address and post code, previous address and postcode, Pension details, Pension scheme provider, employment history, pension benefit illustration currently or on retirement (as appropriate). See View data model | Standards | UK Pensions Dashboards Programme for further details

Description	Details
	Name and business contact details of Provider Personnel and any directors, officers, employees, agents, consultants and contractors of Customer engaged in the performance of the Customer's duties under this Contract).
Categories of Data Subject	Active and Deferred NHS Pension Members, Staff of Customer and customer ~(including agents volunteers and temporary workers), users of the Pensions Dashboard website service
Plan for return and destruction of the data once the Processing is complete UNLESS requirement under law to preserve that type of data	On exit, the Customer's data will be deleted from the ISP when the contract ends, or before if requested by the Customer. The Customer's data held in the ISP is a copy of data already held by the Customer and therefore the Provider shall delete and not return any such copy. Upon request, the Provider will provide the Customer with copies of the Dashboard matching rules that have been used for the Customer's data during the shorter of the duration of the contract and six years so that the Customer may satisfy any requirement from the regulator to retrospectively audit those rules. .
Locations at which the Provider and/or its Sub-contractors process Personal Data under this Contract and international transfers and legal gateway	The Customer agrees to the Provider appointing the following sub-processors: [redacted]
Protective Measures that the Provider and, where applicable, its Sub-contractors have implemented to protect Personal	Details of protective measures that have been implemented will be included by the Provider and will align with information security measures agreed at the Security Schedule of the order form, and Code of connection | Standards | UK Pensions Dashboards Programme

Description	Details
Data processed under this Contract Agreement against a breach of security (insofar as that breach of security relates to data) or a Data Loss Event	