DATA PROTECTION ADDENDUM

between

Paisley Housing Association a Scottish Charity (Scottish Charity Number SCO35589), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2171 and having their Registered Office at Assurance House, 2 Lawn Street, Paisley, PA1 1HA (the "Association");

and

#*[Insert organisation name, a Company]* registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at #[*address]*] (the "Processor")

(each a "**Party**" and together the "**Parties**")

WHEREAS

(a) The Association and the Processor have entered in to an agreement/ contract to #[insert detail] (hereinafter the "Principal Agreement");

(b) This Data Protection Addendum forms part of the Principal Agreement and

(c) In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. **Definitions**

1.1 The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement shall remain in full force and effect. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

    1.1.1 **"Applicable Laws"** means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Association Personal Data in

respect of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Association Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Association pursuant to or in connection with the Principal Agreement/Contract;

1.1.3 "**Contracted Processor**" means Processor or a Subprocessor;

1.1.4 "**Data Protection Laws**" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**EU Data Protection Laws**" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;

1.1.7 "**GDPR**" means EU General Data Protection Regulation 2016/679;

1.1.8 "**Restricted Transfer**" means:

1.1.8.1 a transfer of Association Personal Data from the Association to a Contracted Processor; or

1.1.8.2 an onward transfer of Association Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.9 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Association pursuant to the Principal Agreement/ Contract;

1.1.10 "**Subprocessor**" means any person (including any third party and any , but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor which is engaged in the Processing of Personal Data on behalf of the Association in connection with the Principal Agreement/Contract; and

1.2 The terms, "**Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Personal Data Breach", "Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.3   The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2.   Processing of Association Personal Data

2.1   The Processor shall:

2.1.1   comply with all applicable Data Protection Laws in the Processing of Association Personal Data; and

2.1.2   not Process Association Personal Data other than on the Association's documented instructions unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the relevant Processing of that Personal Data.

2.2   The Association

2.2.1   Instructs the Processor (and authorises Processor to instruct each Subprocessor) to:

2.2.1.1   *Process Association Personal Data; and*

2.2.1.2   *in particular, transfer Association Personal Data to any country or territory,*

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement/Contract; and

2.2.2   warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.

2.3   The Schedule to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Association Personal Data as required by article 28(3) of the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). The Association may make reasonable amendments to the Schedule by written notice to Processor from time to time as the Association reasonably considers necessary to meet those requirements. Nothing in the Schedule (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

3. Processor and Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Association Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Association Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 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, the Processor shall in relation to the Association Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. **Subprocessing**

5.1 The Association authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Subprocessors already engaged by the Processor as at the date of this Addendum, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 The Processor shall give the Association prior written notice of its intention to appoint a Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. The Processor shall not appoint (nor disclose any Association Personal Data to) the proposed Subprocessor except with the prior written consent of the Association.

5.4 With respect to each Subprocessor, the Processor or the relevant shall:

5.4.1 before the Subprocessor first Processes Association Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level

of protection for Association Personal Data required by the Principal Agreement;

5.4.2   ensure that the arrangement between on the one hand (a) the Processor, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Association Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;

5.4.3   if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Processor or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Association Personal Data; and

5.4.4   provide to the Association for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as the Association may request from time to time.

5.5   The Processor shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Association Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of the Processor.

6.   Data Subject Rights

6.1   Taking into account the nature of the Processing, the Processor shall assist the Association by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Association's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2   The Processor shall:

6.2.1   promptly notify the Association if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Association Personal Data; and

6.2.2   ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Association or as required by Applicable Laws to which the Contracted Processor is subject, in which

case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the Contracted Processor responds to the request.

7. **Personal Data Breach**

7.1   The Processor shall notify the Association without undue delay upon the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting the Association Personal Data, providing the Association with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2   The Processor shall co-operate with the Association and at its own expense take such reasonable commercial steps as are directed by the Association to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. **Data Protection Impact Assessment and Prior Consultation**

The Processor shall provide reasonable assistance to the Association with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Association reasonably considers to be required by article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Association Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. **Deletion or return of Association Personal Data**

9.1   Subject to sections 9.2 and 9.3, the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing of Association Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2   Subject to section 9.3, the Association may in its absolute discretion by written notice to the Processor within seven (7) days of the Cessation Date require the Processor to (a) return a complete copy of all Association Personal Data to the Association by secure file transfer in such format as is reasonably notified by the Association to the Processor; and (b) delete and procure the deletion of all other copies of Association Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.

9.3   Each Contracted Processor may retain Association Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4   Processor shall provide written certification to the Association that it has fully complied with this section 9 within fourteen (14) days of the Cessation Date.

10.   Audit rights

10.1   Subject to sections 10.2 and 10.3, the Processor shall make available the Association on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Association or an auditor mandated by the Association in relation to the Processing of the Association Personal Data by the Contracted Processors.

10.2   Information and audit rights of the Association only arise under section 10.1 to the extent that the Principal Agreement/Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).

10.3   Where carrying out an audit of Personal Data, the Association shall give the Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1   to any individual unless they produce reasonable evidence of identity and authority; or

10.3.2   outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Association undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins

11.   General Terms

Governing law and jurisdiction

11.1   The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.2   this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement.

Order of precedence

11.3   Nothing in this Addendum reduces the Processor's obligations under the Principal Agreement in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement.

11.4   Subject to section 11.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

Changes in Data Protection Laws, etc.

11.5   The Association may:

11.5.1   by giving at least twenty eight (28) days' written notice to the Processor, from time to time make any variations to the terms of the Addendum which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

11.5.2   propose any other variations to this Addendum which the Association reasonably considers to be necessary to address the requirements of any Data Protection Law.

Severance

11.6   Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as

possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

On behalf of Paisley Housing Association

at Assurance House, 2 Lawn Street, Paisley, PA1 1HA

on

by

_____   _____
Print Full Name   Authorised Signatory

before this witness

_____   _____
Print Full Name   Witness

Address

Assurance House,

2 Lawn Street
_____

Paisley, PA1 1HA
_____

_____
On behalf of the Processor

at

on

by

_____   _____

Print Full Name   Director/Secretary/Authorised
                                   Signatory

before this witness

_____   _____
Print Full Name   Witness

Address

_____

_____

_____

SCHEDULE

This is the Schedule referred to in the foregoing Data Protection Addendum between the Association and the Processor