Hillhead
HOUSING ASSOCIATION
Building on progress for a brighter Hillhead

DATA PROTECTION ADDENDUM

Between

Hillhead Housing Association 2000, a Scottish Charity (Scottish Charity Number SC029908), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2562R(S) and having their Registered Office at 2 Meiklehill Road, Hillhead, Kirkintilloch G66 2LA (the “Association”)

and

#[Insert organisation name and address (the "Processor”)
(each a "**Party**" and together the "**Parties**")

WHEREAS

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

(b) This Data Protection Addendum forms part of the Principal Contract; 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 Contract. Except as modified below, the terms of the Principal Agreement/Contract 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 "**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 Contract;

1.1.2 "**Data Protection Laws**" means the Data Protection Act 1998, the General Data Protection Regulation 2016/679 and all relative European Union and Member State data protection legislation in force and as amended or replaced from time to time.

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

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

1.1.5 "**Restricted Transfer**" means:

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

1.1.5.2 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);

1.1.6 "**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 Contract;

1.1.7 "**Subprocessor**" means any person (including any third party, but excluding an employee of the 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.

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

The parties hereby and acknowledge that the information contained in Schedule 1 is an accurate description of the Processing of data to be carried out.

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;

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

2.1.3 inform the Controller immediately if, in its opinion, an instruction from the Controller infringes any obligation under Data Protection Laws

2.1.4 maintain written records, including in electronic form, of all Processing activities carried out in performance of the processing of the Services or otherwise on behalf of the Controller containing the information set out in Article 30(2) of the General Directive on Data Protection 2016/679 (GDPR); and

2.1.5 provide the Controller with details of the Processor's Data Protection Officer or other designated individual with responsibility for data protection.

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 Contract provided that a data transfer risk assessment has been carried out and the appropriate EU model clauses have been completed and signed by the appropriate parties or other appropriate safeguards have been put in place prior to any such data transfer taking place; 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.

3. Processor and Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of the 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 Data Protection 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 Contract.

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 the Processor and 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 the Processor and the Subprocessor, before the Subprocessor first Processes Association Personal Data; and

5.4.4 provide to the Association for review such copies of the Processor's 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 Processor does not respond to that request except on the documented instructions of the Association or as required by law, in which case the Processor shall to the extent permitted by law inform the Association of that legal requirement before the 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 Association 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 The Processor may retain Association Personal Data to the extent required by law and only to the extent and for such period as required by law and always provided that the Processor shall ensure the confidentiality of all such Association Personal Data and shall ensure that such Association Personal Data is only Processed required by law and for no other purpose.

9.4 The 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 Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. The 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. Indemnity

The Processor shall indemnify and keep the Association indemnified against all losses, claims, damages, liabilities, fines, interest, penalties, costs, charges, sanctions, expenses, compensation paid to Data Subjects, demands and legal and other professional costs (calculated on a full indemnity basis and, in each case, whether or not arising from any investigation by, or imposed by, the Information Commissioner's Office (or other Supervisory Authority) arising out of or in connection with any breach by the Contracted Processor of its obligations under this Addendum and all amounts paid or payable by the Association to a third party which would not have been paid or payable if the Contracted Processor's breach of this Addendum had not occurred.

12. General Terms

Governing law and jurisdiction

12.1 This Addendum shall be governed by and construed in accordance with the law of Scotland and the Parties hereby submit to the exclusive jurisdiction of the Scottish Courts in respect of any dispute or claim arising out of or in connection with it or its subject matter or formation.

Order of precedence

12.2 Nothing in this Addendum reduces the Processor's obligations under the Principal Agreement/Contract 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 Contract.

12.3 In the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement/Contract 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.

12.4 The Association may:

12.4.1 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

12.4.2 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

12.5 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.

Term and Termination

11.6 This Agreement shall continue in full force and effect for the duration of the Principal Contract. For the avoidance of doubt, this Addendum shall terminate automatically on termination of the Principal Contract.

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 the Association

at

on

by

______________________________	______________________________
Print Full Name	Director/Secretary/Authorised Signatory

before this witness

______________________________	______________________________
Print Full Name	Witness

Address

____

____

____

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

- **Subject matter and duration of processing**
- **Nature and purposes of processing**
- **Types of Personal Data to be processed and Categories of Data Subjects**