DATA PROCESSING AGREEMENT

THIS AGREEMENT is made the [insert day] of [insert month and year].

BETWEEN:

(1) **Cadarn Housing Group Limited**, a Registered Society under the Co-operative and Community Benefit Societies Act 2014, registration number **21180R,** registered office at **5 Village Way, Tongwynlais, Cardiff, CF15 7NE** ("Controller") and

(2) **[insert Processor Entity],** a company registered in the United Kingdom under number [**insert registered number**], whose registered office is at [**insert registered address**] ("Processor").

WHEREAS:

(1) Under an agreement between the Controller and the Processor ("the Service Agreement") the Processor provides to the Controller the Services described in Schedule 1.

(2) The provision of the Services by the Processor involves it in processing the Personal Data described in Schedule 2 on behalf of the Controller.

(3) Under Article 28(3) UK General Data Protection Regulation ("UK GDPR"), the Controller is required to put in place an agreement in writing between the Controller and any organisation which processes Personal Data on its behalf governing the processing of that data.

(4) The Parties have agreed to enter into this Agreement to ensure compliance with the said provisions of the UK GDPR in relation to all processing of the Personal Data by the Processor for the Controller.

(5) The terms of this Agreement are to apply to all processing of Personal Data carried out for the Controller by the Processor and to all Personal Data held by the Processor in relation to all such processing.

IT IS AGREED as follows:

1. Definitions and Interpretation

1.1 In this Agreement, unless the context otherwise requires, the following expressions have the following meanings:

"Controller", "Processor", "processing", and "Data Subject" shall have the meanings given to the terms "controller", "processor", "processing", and "Data Subject" respectively in Article 4 UK GDPR;

"ICO" means the UK's supervisory authority, the Information Commissioner's Office;

“Personal Data” means all such “Personal Data”, as defined in Article 4 of the UK GDPR, as is, or is to be, processed by the Processor on behalf of the Controller, as described in Schedule 2;

“Services” means those services described in Schedule 1 which are provided by the Processor to the Controller and which the Controller uses for the purposes described in Schedule 1;

“Sub-Processor” means a sub-processor appointed by the Processor to process the Personal Data; and

“Sub-Processing Agreement” means an agreement between the Processor and a Sub-Processor governing the Personal Data processing carried out by the Sub-Processor, as described in Clause 9.

1.2 Unless the context otherwise requires, each reference in this Agreement to:

1.2.1 “writing”, and any cognate expression, includes a reference to any communication effected by electronic or facsimile transmission or similar means;

1.2.2 a statute or a provision of a statute is a reference to that statute or provision as amended or re-enacted at the relevant time;

1.2.3 “this Agreement” is a reference to this Agreement and each of the Schedules as amended or supplemented at the relevant time;

1.2.4 a Schedule is a schedule to this Agreement;

1.2.5 a Clause or paragraph is a reference to a Clause of this Agreement (other than the Schedules) or a paragraph of the relevant Schedule; and

1.2.6 a "Party" or the "Parties" refer to the parties to this Agreement.

1.3 The headings used in this Agreement are for convenience only and shall have no effect upon the interpretation of this Agreement.

1.4 Words imparting the singular number shall include the plural and vice versa.

1.5 References to any gender shall include all other genders.

1.6 References to persons shall include corporations.

2. Scope and Application of this Agreement

2.1 The provisions of this Agreement shall apply to the processing of the Personal Data described in Schedule 2, carried out for the Controller by the Processor, and to all Personal Data held or accessed by the Processor in relation to all such processing whether such Personal Data is held at the date of this Agreement or received afterwards.

2.2 The provisions of this Agreement supersede any other arrangement, understanding, or agreement including, but not limited to, the Service Agreement made between the Parties at any time relating to the Personal Data.

2.3 This Agreement shall continue in full force and effect for so long as the Processor is processing Personal Data on behalf of the Controller, and thereafter as provided in Clause 10.

3. Provision of the Services and Processing Personal Data

3.1 The Processor is only to carry out the Services, and only to process the Personal Data received from the Controller:

3.2 for the purposes of those Services and not for any other purpose;

3.3 to the extent and in such a manner as is necessary for those purposes; and

3.4 strictly in accordance with the express written authorisation and instructions of the Controller (which may be specific instructions or instructions of a general nature or as otherwise notified by the Controller to the Processor).

4. Data Protection Compliance

4.1 All instructions given by the Controller to the Processor shall be made in writing and shall at all times be in compliance with the UK GDPR and other applicable laws. The Processor shall act only on such written instructions from the Controller unless the Processor is required by law to do otherwise (as per Article 29 UK GDPR).

4.2 The Processor shall promptly comply with any request from the Controller requiring the Processor to amend, transfer, delete, or otherwise dispose of the Personal Data.

4.3 The Processor shall transfer all Personal Data to the Controller on the Controller's request in the formats, at the times, and in compliance with the Controller's written instructions.

4.4 Both Parties shall comply at all times with the UK GDPR and other applicable laws and shall not perform their obligations under this Agreement or any other agreement or arrangement between themselves in such way as to cause either Party to breach any of its applicable obligations under the UK GDPR.

4.5 The Processor agrees to comply with any reasonable measures required by the Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with any and all applicable legislation from time to time in force (including, but not limited to, the UK GDPR) and any best practice guidance issued by the ICO.

4.6 The Processor shall provide all reasonable assistance to the Controller in complying with its obligations under the UK GDPR with respect to the security of processing, the notification of Personal Data breaches, the conduct of data protection impact assessments, and in dealings with the ICO.

4.7 When processing the Personal Data on behalf of the Controller, the Processor shall:

4.7.1 not process the Personal Data outside the UK or European Economic Area (all EU member states, plus Iceland, Liechtenstein, and Norway) ("EEA") without the prior written consent of the Controller and, where the Controller consents to such a transfer to a country that is outside of the UK or EEA, to comply with the obligations of Processors under the provisions applicable to transfers of Personal Data to third countries set out in Chapter 5 UK GDPR, by providing an adequate level of protection to any Personal Data that is transferred;

4.7.2 not transfer any of the Personal Data to any third party without the written consent of the Controller and, in the event of such consent, the Personal Data shall be transferred strictly subject to the terms of a suitable agreement, as set out in Clause 9;

4.7.3 process the Personal Data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Controller or as may be required by law (in which case, the Processor shall inform the Controller of the legal requirement in question before processing the Personal Data for that purpose unless prohibited from doing so by law);

4.7.4 implement appropriate technical and organisational measures and take all steps necessary to protect the Personal Data against any unauthorised processing, including any accidental or unlawful loss, destruction, damage, alteration, disclosure or access. In assessing the appropriate level of security, the Parties shall take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risks for Data Subjects. The Processor shall at least implement the technical and organisational measures specified in Schedule 3 and shall inform the Controller in advance of any material changes to such measures;

4.7.5 if so requested by the Controller (and within the timescales required by the Controller) supply further details of the technical and organisational systems in place to safeguard the security of the Personal Data held and to prevent unauthorised access;

4.7.6 keep detailed records of all processing activities carried out on the Personal Data in accordance with the requirements of Article 30(2) UK GDPR;

4.7.7 make available to the Controller any and all such information as is reasonably required and necessary to demonstrate the Processor's compliance with the UK GDPR;

4.7.8 on reasonable prior notice, submit to audits and inspections and provide the Controller with any information reasonably required in order to assess and verify compliance with the provisions of this Agreement and both Parties' compliance with the requirements of the UK GDPR. The requirement to give notice will not apply if the Controller believes that the Processor is in breach of any of its obligations under this Agreement or under the law; and

4.7.9 inform the Controller immediately if it is asked to do anything that infringes the UK GDPR or any other applicable data protection legislation.

5. Data Subject Access, Complaints, and Breaches

5.1 The Processor shall assist the Controller in complying with its obligations under the UK GDPR. In particular, the following shall apply to Data Subject access requests, complaints, and data breaches.

5.2 The Processor shall notify the Controller without undue delay if it receives:

5.2.1 a subject access request from a Data Subject; or

5.2.2 any other complaint or request relating to the processing of the Personal Data.

5.3 The Processor shall cooperate fully with the Controller and assist as required in relation to any subject access request, complaint, or other request, including by:

5.3.1 providing the Controller with full details of the complaint or request;

5.3.2 providing the necessary information and assistance in order to comply with a subject access request;

5.3.3 providing the Controller with any Personal Data it holds in relation to a Data Subject (within the timescales required by the Controller); and

5.3.4 providing the Controller with any other information requested by the Controller.

5.4 The Processor shall notify the Controller immediately if it becomes aware of any form of Personal Data breach, including any unauthorised or unlawful processing, loss of, damage to, or destruction of any of the Personal Data.

6. Liability and Indemnity

6.1 The Processor shall indemnify, keep indemnified and defend the Controller, at the Processor's own expense, against all claims, liabilities, costs, expenses, damages and losses (including all interest, penalties and legal costs (calculated on a full indemnity basis) and all other professional costs and expenses) suffered or incurred by the Controller arising out of the failure by the Processor or its employees or agents to comply with any of its obligations under this Agreement ("Claims"). Each party acknowledges that Claims include any claim or action brought by a Data Subject arising from the Supplier's breach of its obligations under this Agreement.

7. Intellectual Property Rights

7.1 All copyright, database rights, and other intellectual property rights subsisting in the Personal Data (including but not limited to any updates, amendments, or adaptations to the Personal Data made by either the Controller or the Processor) shall belong to the Controller or to any other applicable third party from whom the Controller has obtained the Personal Data under licence (including, but not limited to, Data Subjects, where applicable). The Processor is licensed to use such Personal Data under such rights only for the purposes of the Services, and in accordance with this Agreement.

8. Confidentiality

8.1 The Processor shall maintain the Personal Data in confidence, and in particular, unless the Controller has given written consent for the Processor to do so, the Processor shall not disclose any Personal Data supplied to the Processor by, for, or on behalf of, the Controller to any third party. The Processor shall not process or make any use of any Personal Data supplied to it by the Controller otherwise than in connection with the provision of the Services to the Controller.

8.2 The Processor shall ensure that all personnel who are to access and/or process any of the Personal Data are contractually obliged to keep the Personal Data confidential.

8.3 The obligations set out in in this Clause 8 shall continue for a period of six years after the cessation of the provision of Services by the Processor to the Controller.

8.4 Nothing in this Agreement shall prevent either Party from complying with any requirement to disclose Personal Data where such disclosure is required by law. In such cases, the Party required to disclose shall notify the other Party of the disclosure requirements prior to disclosure, unless such notification is prohibited by law.

9. Appointment of Sub-Processors

9.1 The Processor shall not sub-contract any of its obligations or rights under this Agreement without the prior written consent of the Controller (such consent not to be unreasonably withheld).

9.2 In the event that the Processor appoints a Sub-Processor (with the written consent of the Controller), the Processor shall:

9.2.1 enter into a Sub-Processing Agreement with the Sub-Processor which shall impose upon the Sub-Processor the same obligations as are imposed upon the Processor by this Agreement and which shall permit both the Processor and the Controller to enforce those obligations; and

9.2.2 ensure that the Sub-Processor complies fully with its obligations under the Sub-Processing Agreement and the UK GDPR.

9.3 In the event that a Sub-Processor fails to meet its obligations under any Sub-Processing Agreement, the Processor shall remain fully liable to the Controller for failing to meet its obligations under this Agreement.

10. Deletion and/or Disposal of Personal Data

10.1 The Processor shall, at the written request of the Controller, delete (or otherwise dispose of) the Personal Data or return it to the Controller in the format(s) reasonably requested by the Controller within a reasonable time after the earlier of the following:

10.1.1 the end of the provision of the Services; or

10.1.2 the processing of that Personal Data by the Processor is no longer required for the performance of the Processor's obligations under this Agreement or the Service Agreement.

10.2 Following the deletion, disposal, or return of the Personal Data under sub-Clause 10.1, the Processor shall delete (or otherwise dispose of) all further copies of the Personal Data that it holds, unless retention of such copies is required by law, in which case the Processor shall inform the Controller of such requirement(s) in writing.

11. Law and Jurisdiction

11.1 This Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall be governed by, and construed in accordance with, the laws of England and Wales.

11.2 Any dispute, controversy, proceedings or claim between the Parties relating to this Agreement (including any non-contractual matters and obligations arising therefrom or associated therewith) shall fall within the jurisdiction of the courts of England and Wales.

SIGNED for and on behalf of the Controller by:

[insert name]

Authorised Signature

Date: [insert date]

SIGNED for and on behalf of the Processor by:
[insert name]

Authorised Signature

Date: [insert date]

SCHEDULE 1

Services

Provision of reactive pest control services across residential properties and communal areas managed by Cadarn Housing Group, including attendance, treatment, diagnostic reporting, minor enabling works, and associated advisory services, as further described in the Specification (Schedule 3 of the Service Agreement).

SCHEDULE 2

Personal Data to be processed

Type of Personal Data	Category of Data Subject	Nature of Processing Carried Out	Purpose(s) of Processing	Retention Period	Duration of Processing
Name, address, phone number	Tenants and residents	Access, use, storage, transmission	Delivery of reactive pest control services and enabling works	Duration of contract plus 3 years	For the term of the Service Agreement
Contact warning notes (operational flags re: access, communication preferences, vulnerability indicators)	Tenants and residents	Access, use on a job-by-job basis	To inform safe and appropriate service delivery at individual properties	Duration of contract plus 3 years	For the term of the Service Agreement
Visit reports including root cause categorisation and photographic evidence	Tenants and residents	Creation, storage, transmission to Controller	Reporting on pest control attendances and enabling identification of repairs and recharges	Duration of contract plus 3 years	For the term of the Service Agreement

SCHEDULE 3

Technical and organisational measures to ensure the security of Personal Data

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 risks to Data Subjects, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The Processor shall implement the following, as appropriate:

   - the pseudonymisation and encryption of the Personal Data;
   - the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   - the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
   - a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

3. As a minimum, the Processor shall implement the items set out below.

   Organisational Measures
   The Processor shall implement the following policies:

   - Data Protection Policy
   - Information Security Policy
   - Data Subjects’ Rights Policy
   - Personal Data Breach Policy
   - Clear Desk and Clear Screen Policy
   - Password Management Policy
   - Access Control Policy
   - Mobile Devices Policy
   - Acceptable Use Policy

The Processor shall ensure all personnel that process or have access to Personal Data have data protection awareness training upon induction and regular refresher training thereafter.

Technical Measures

The Processor shall implement the following measures, as appropriate:

- Firewalls
- Anti-malware
- Encryption of Personal Data
- Access controls