PRIVACY POLICY

Last approved by Management Committee: 5 August 2020

Date for Review: August 2023

The information in this document is available in other languages or on tape/CD, in large print and also in Braille.
For details contact the Association on
0141 578 0200 or e-mail: admin@hillheadhousing.org

本文件所載資料備有中文 (廣東話) 版本，也可以製作成錄音帶/光碟，以及利用特大字體和凸字印製，以供索取。
欲知有關詳情，請聯絡本協會，電話：0141 578 0200，或向我們發送電郵， 電郵地址：admin@hillheadhousing.org

Tha am fiosrachadh anns an sgrìobhainn seo ri fhaotainn ann an Gàidhlig no air teip/CD, sa chlò mhòr agus cuideachd ann an Clò nan Dall.
Airson tuilleadh fiosrachaidh, cuiribh fios dhan Chomann air 0141 578 0200 no cuiribh post-dealain gu: admin@hillheadhousing.org

इस दस्तावेज़ में दी गई जानकारी हिन्दी में भी या टेप, सी डी, बड़ी छाप और ब्रैल में भी उपलब्ध है। विवरण के लिए ऐसोसिएशन को नम्बर 0141 578 0200 पर या ई-मेल के द्वारा सम्पर्क करें : admin@hillheadhousing.org

ਇਸ ਦਸਤਾਵੇਜ਼ ਵਿਚ ਦਿੱਤੀ ਗਈ ਜਾਣਕਾਰੀ ਪੰਜਾਬੀ ਵਿੱਚ ਵੀ ਜਾਂ ਟੇਪ, ਸੀ ਡੀ, ਵੱਡੀ ਛਪਾਈ ਅਤੇ ਬ੍ਰੈਲ 'ਤੇ ਵੀ ਉਪਲਬਧ ਹੈ। ਵੇਰਵੇ ਲਈ ਐਸੋਸਿਏਸ਼ਨ ਨੂੰ ਨੰਬਰ 0141 578 0200 'ਤੇ ਜਾਂ ਈ-ਮੇਲ ਰਾਹੀਂ ਸੰਪਰਕ ਕਰੋ : admin@hillheadhousing.org

اس دستاویز میں درج معلومات اُردو زبان یا آڈیوٹیپ / سی ڈی، بڑی طباعت اور بریل میں بھی دستیاب ہیں۔
تفصیلات کے لئے ایسوسی ایشن سے ٹیلیفون نمبر **0141 578 0200** یا ای میل **admin@hillheadhousing.org**
کے ذریعے رابطہ قائم کریں۔

Regulatory Compliance	Standard 2 The RSL is open about and accountable for what it does. It understands and takes account of the needs and priorities of its tenants, service users and stakeholders. And its primary focus is the sustainable achievement of these priorities.
Financial Impact	Medium, in the event of any fines
Risk Assessment	Medium, in the event of any breach

Contents

1. Introduction

Hillhead Housing Association 2000 is committed to ensuring the secure and safe management of data it holds in relation to customers, staff and other individuals. Hillhead Housing Association 2000's staff members have a responsibility to ensure compliance with the terms of this policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

Hillhead Housing Association 2000 needs to gather and use certain information about individuals. These can include customers (tenants, factored owners, etc.), employees and other individuals that Hillhead Housing Association 2000 has a relationship with. Hillhead Housing Association 2000 manages a significant amount of information, from a variety of sources. This information contains 'Personal Data' and 'Sensitive Personal Data' (known as "Special Category" personal data under the GDPR).

This policy sets out Hillhead Housing Association 2000's duties in processing that data, and the purpose of this policy is to set out the procedures for the management of such data.

2. Legislation

It is a legal requirement that Hillhead Housing Association 2000 process data correctly; Hillhead Housing Association 2000 must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

(a) the General Data Protection Regulation ("the GDPR");
(b) the Privacy and Electronic Communications Regulations 2003 ("the PECRs" (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
(c) The Data Protection Act 2018 (DPA2018)

3. Data

Hillhead Housing Association 2000 holds a variety of information relating to individuals, including customers and employees (also referred to as data subjects) which is known as "personal data". The personal data held and processed by Hillhead Housing Association 2000 is detailed within the Privacy Notice at **Appendix 1**.

Separate Privacy Notices are provided to Staff, Committee Members and a version is also published on our website.

3.1 "Personal data" is that from which a living individual can be identified either by that data alone or in conjunction with other data held by Hillhead Housing Association 2000.

3.2 Hillhead Housing Association 2000 also holds personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Processing of personal data

4.1 Hillhead Housing Association 2000 is permitted to process personal data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the **consent** of the data subject (see section 4.4);
- Processing is necessary for the performance of a **contract** between Hillhead Housing Association 2000 and the data subject or for entering into a contract with the data subject;
- Processing is necessary for Hillhead Housing Association 2000's compliance with a **legal obligation**;
- Processing is necessary to protect the **vital interests** of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the **public interest** or in the exercise of Hillhead Housing Association 2000's official authority; or
- Processing is necessary in the support of the **legitimate interests** of Hillhead Housing Association 2000 or other third party.

4.2 Privacy Notice

Hillhead Housing Association 2000 has produced a Privacy Notice which it is required to provide to all people whose personal data is held by Hillhead Housing Association 2000. The Privacy Notice must be provided to the person from the outset of processing their personal data and they should be advised of the terms of the Privacy Notice when it is provided to them.

The Privacy Notice (at **Appendix 1**) sets out the personal data processed by Hillhead Housing Association 2000 and the basis for that processing. This document is provided to all of Hillhead Housing Association 2000's customers at the outset of processing their data.

4.3 Employees

Employee personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by Hillhead Housing Association 2000.

Details of the data held, and processing of that data is contained within the Employee Privacy Notice which is provided to Employees at the same time as their Contract of Employment.

A copy of any employee's personal data held by Hillhead Housing Association 2000 is available upon request by that employee from the Head of Corporate Services.

4.4 Consent

Consent as a ground for processing might be required to be used from time to time by Hillhead Housing Association 2000 when processing personal data. It should be used by Hillhead Housing Association 2000 where no other alternative ground for processing is available. In the event that Hillhead Housing Association 2000 requires to obtain consent to process a data subject's personal data, it will obtain that consent in writing.

The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form if willing to consent. Any consent to be obtained by Hillhead Housing Association 2000 must be for a *specific and defined purpose* (i.e. general consent cannot be sought).

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that Hillhead Housing Association 2000 processes Special Category Personal Data or Sensitive Personal Data, it must do so in accordance with one of the following grounds of processing:

- The data subject has given **explicit consent** to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to **employment or social security**;
- Processing is necessary to protect the **vital interest** of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of **legal claims**, or whenever court are acting in their judicial capacity; and Processing is necessary for reasons of **substantial public interest**.

5. Data sharing

Hillhead Housing Association 2000 shares its data with various third parties for numerous reasons in order that its day-to-day activities are carried out in accordance with Hillhead Housing Association 2000's relevant policies and procedures.

5.1 In order that Hillhead Housing Association 2000 can monitor compliance by these third parties with Data Protection laws, Hillhead Housing Association 2000 will require the third party organisations to enter into an Agreement with Hillhead Housing Association 2000 governing the processing of data, security measures to

be implemented and responsibility for breaches. This is achieved via Data Processing Agreements.

5.2 Personal data is from time to time shared amongst Hillhead Housing Association 2000 and third parties who require to process personal data that Hillhead Housing Association 2000 is also having to process. Both Hillhead Housing Association 2000 and the third party will be processing that data in their individual capacities as data controllers.

5.3 Where Hillhead Housing Association 2000 shares in the processing of personal data with a third party organisation (for example, for processing of the employees' pension), it will require the third party organisation to enter into a Data Sharing Agreement with Hillhead Housing Association 2000 in accordance with the terms of the model Data Sharing Agreement set out in **Appendix 2** to this policy.

5.4 Data processors

A data processor is a third party entity that processes personal data on behalf of Hillhead Housing Association 2000 and is frequently engaged in areas where Hillhead Housing Association 2000's work is outsourced (for example, payroll, maintenance and repair works).

A data processor must comply with Data Protection laws. Hillhead Housing Association 2000's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify Hillhead Housing Association 2000 if a data breach is suffered.

If a data processor wishes to sub-contact their processing, prior written consent of Hillhead Housing Association 2000 must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors. Where Hillhead Housing Association 2000 contracts with a third party to process personal data held by Hillhead Housing Association 2000, it will require the third party to enter into a Data Protection Addendum with Hillhead Housing Association 2000 in accordance with the terms of the model Data Protection Addendum set out in **Appendix 3** to this Policy.

6. Data storage and security

All personal data held by Hillhead Housing Association 2000 must be stored securely, whether electronically or in paper format.

6.1 Paper storage

If personal data is stored on paper it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no personal data is left where unauthorised personnel can access it. When the personal data is no longer required it must be disposed of by the employee so as to ensure its destruction.

If the personal data is required to be retained on a physical file, the employee should ensure that it is affixed to the file which is then stored in accordance with Hillhead Housing Association 2000's storage provisions.

6.2 Electronic storage

Personal data stored electronically must also be protected from unauthorised use and access. Personal data should be password protected when being sent internally or externally to Hillhead Housing Association 2000's data processors or those with whom Hillhead Housing Association 2000 has entered into a Data Sharing Agreement.

If personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be both encrypted and stored securely at all times when not being used. Personal data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

7. Breaches

A data breach can occur at any point when handling personal data and Hillhead Housing Association 2000 has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects are required to be reported externally to the Information Commissioner's Office (ICO) in accordance with section 7.2.

7.1 Internal reporting

Hillhead Housing Association 2000 takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six hours after it has occurred, the DPO must be notified of:

  (i) the breach;
  (ii) how it occurred;
  (iii) what the likely impact of that breach is on any data subject(s);

- Hillhead Housing Association 2000 must seek to contain the breach by whatever means available;
- The DPO must consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with this section 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

7.2 Reporting to the ICO

The DPO will report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the ICO within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data Protection Officer (DPO)

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by Hillhead Housing Association 2000 with Data Protection laws. Hillhead Housing Association 2000 has elected RGDP LLP (www.rgdp.co.uk) to act as our Data Protection Officer. To contact them, please email info@rgdp.co.uk
Please also copy us in at: admin@hillheadhousing.org

The DPO will be responsible for:

- monitoring Hillhead Housing Association 2000's compliance with Data Protection laws and this policy
- co-operating with and serving as Hillhead Housing Association 2000's contact for discussions with the ICO
- reporting breaches or suspected breaches to the ICO and data subjects in accordance with **Section 7** above

9. Data subject rights

Certain rights are provided to data subjects under the GDPR. Data subjects are entitled to view the personal data held about them by Hillhead Housing Association 2000, whether in written or electronic form. Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to Hillhead Housing Association 2000's processing of their data. These rights are notified to Hillhead Housing Association 2000's tenants and other customers in Hillhead Housing Association 2000's Privacy Notice.

9.1 Subject Access Requests

Data subjects are permitted to view their data held by Hillhead Housing Association 2000 upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, Hillhead Housing Association 2000 must respond to the Subject Access Request within one month of the date of receipt of the request. Hillhead Housing Association 2000:

- must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law
- where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request, or

- where Hillhead Housing Association 2000 does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

9.2 The right to be forgotten

In certain circumstances, a data subject can exercise their right to be forgotten by submitting a request in writing to Hillhead Housing Association 2000 seeking that Hillhead Housing Association 2000 erase the data subject's personal data in its entirety.

Each request received by Hillhead Housing Association 2000 will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with this section and will respond in writing to the request.

9.3 The right to restrict or object to processing

A data subject may request that Hillhead Housing Association 2000 restrict its processing of the data subject's personal data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by Hillhead Housing Association 2000, a data subject has an absolute right to object to processing of this nature by Hillhead Housing Association 2000, and if Hillhead Housing Association 2000 receives a written request to cease processing for this purpose, then it must do so immediately.

Each request received by Hillhead Housing Association 2000 will require to be considered on its own merits. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with clause 9.3 and will respond in writing to the request.

10. Data Protection Impact Assessments (DPIAs)

These are a means of assisting Hillhead Housing Association 2000 in identifying and reducing the risks that our operations have on personal privacy of data subjects.
Hillhead Housing Association 2000 will:

- Carry out a DPIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new ICT system for storing and accessing personal data; and
- In carrying out a DPIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks

identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data

Hillhead Housing Association 2000 will require to consult the ICO in the event that a DPIA identifies a high level of risk which cannot be reduced. The Data Protection Officer will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA they will be required to notify the DPO within five working days.

11. Archiving, retention and destruction of data

Hillhead Housing Association 2000 cannot store and retain personal data indefinitely. It must ensure that personal data is only retained for the period necessary. Hillhead Housing Association 2000 shall ensure that all personal data is archived and destroyed in accordance with the periods specified within the published Data Retention Policy and Schedule.

APPENDIX 1 – PRIVACY NOTICE

Hillhead Housing Association

CUSTOMER PRIVACY NOTICE

(How we use your personal information)

This notice explains what information we collect, when we collect it and how we use this. During the course of our activities, we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Who are we?

Hillhead Housing Association 2000, registered as:

A Scottish Charity (Scottish Charity Number SC029908);
A registered society under the Co-operative and Community Benefit Societies Act 2014;
With the Financial Services Agency with Registered Number 2562RS;
With the Scottish Housing Regulator with Registration Number 326

and having their Registered Office at:

2 Meiklehill Road, Hillhead, Kirkintilloch, G66 2LA

Hillhead Housing Association 2000 takes the issue of security and data protection very seriously and strictly adheres to guidelines published in the General Data Protection Regulation applicable from the 25 May 2018 and the Data Protection Act 2018

We are notified as a Data Controller with the Office of the Information Commissioner ICO) under registration number Z8278640 and we are the data controller of any personal data that you provide to us.

How we collect information from you and what information we collect

We collect information about you:

- when you apply for housing with us, become a tenant, request services/ repairs, enter into a factoring agreement with ourselves howsoever arising or otherwise provide us with your personal details
- when you apply to become a member;
- from your use of our online services, whether to report any tenancy/ factor related issues, make a complaint or otherwise;
- from your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information);
- when you are a member of a scrutiny panel;

We may collect the following information about you:

- Personal details: name, addresses, date of birth
- Contact details: home phone number, mobile phone number and email address
- Further details: NI number, gender, ethnicity, disability, medical details, marital status,
- Signature, unacceptable behaviour warnings, criminal activity
- Household composition: details of existing accommodation arrangements and family
- members seeking accommodation with the applicant
- Tenancy Details: start and end dates, rent paid, under/over payments, arrears
- Payment details: bank account details, 3rd party payment details
- Repairs: repairs requested, access details, completion dates
- Share membership number
- Purchase details: solicitors details
- Employment: benefit/council tax status and payments, employment history, education
- history, tax code, trade union membership
- Employment application details, asylum status, criminal record declaration
- Location: IP address when you access our website
- Images: photo identification and CCTV images

We may also record factual information whenever you contact us or use our services, as well as information about other action we take, so that we have an accurate record of what happened.

We may receive the following information from third parties:

- Benefits information, including awards of Housing Benefit/Universal Credit;
- Payments made by you to us;
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland, Social Services and/or Local Authorities;
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour
- Medical reports for medical adaptations and Social Work reports for applications;
- Tracing and Employment details from debt collection agencies;
- Title Deeds

Why we need this information about you and how it will be used

We need your information and will use your information to:

- Undertake and perform our obligations and duties to you in accordance with the terms of our contract with you;
- Enable us to supply you with the services and information that you have requested;
- Enable us to respond to your repair request, housing application and complaints made;
- Analyse the information we collect so that we can administer, support, improve and develop our business and the services we offer;
- Contact you in order to send you details of any changes to our or suppliers that may affect you;
- Progress all other purposes consistent with the proper performance of our operations and business; and
- Contact you for your views on our products and services.

Sharing of your information

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK / EEA. We may disclose your information to other third parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- If we enter into a joint venture with or merge with another business entity, your information may be disclosed to our new business partners or owners;
- If we instruct repair or maintenance works, your information may be disclosed to any contractor;
- If we are investigating a complaint, information may be disclosed to Police Scotland, Local Authority / Council and/or Council Departments, Scottish Fire & Rescue Service and others involved in any complaint, *whether investigating the complaint or otherwise*;
- If we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and Local Authority / Council and/or Council departments);
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority / Council and/or Council Departments and the Department of Work & Pensions;

- We may share details with our Data Protection Team and/or Legal Advisors
- If we are conducting a survey of our products and/or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results;
- If you are using an advice or advocacy service (such as a solicitor, advice agency or the welfare benefits advisor based in Hillhead Housing Association 2000's Office) we will share relevant information with them where it is necessary to progress your case.
- If you request that we share your information with other RSLs who may assist in re-housing you.
- If your household is threatened with homelessness, your information may be shared between us and Local Health Authority and Social Care Partnership(s).
- If we are pursuing debts associated with a tenancy or a former tenancy we may share your basic information with a third party agency to assist in the recovery of those debts;
- If we are making an insurance claim following an incident we may share your information with our insurers.
- If we are being audited then we may share your information with our auditors.
- Where there is a legal action that involves you such as action to recover a tenancy your information may be shared with a solicitor to assist in the legal process.
- To fulfil our legal and regulatory obligations to bodies such as the Scottish Housing Regulator, Financial Conduct Authority or the Office of the Scottish Charity Regulator.

Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Transfers outside the UK and Europe

Your information will only be stored within the UK and EEA.

Security

When you give us information, we take steps to make sure that your personal information is kept secure and safe. All information is kept in line with our Privacy Policy which is available on our website or from reception.

Only Hillhead Housing Association 2000 staff and partners and contractors who have signed data sharing agreements and who need to see your personal information will have access to it.

We will not usually retain your payment details unless you make payments to us using Direct Debit.

Our computer systems are located in our main office, however our staff may occasionally use laptops, tablet or other devices offsite, i.e. for homeworking. In instances where devices are used remotely this will be secure and under strict control at all times. Additionally, we have the following controls in place to ensure the security of your personal information:

- All paper based records are securely locked in storage cupboards when not actively being Used.
- Our offices are protected by an alarm system, a security company and are monitored by CCTV.
- All Hillhead Housing Association 2000 computer servers are within a secure network

- Systems are password protected, patch updates to our servers are implemented and we regularly review system access rights.
- All electronic communication takes place within this secure environment.

The unauthorised use of IT systems is prevented by:

- User ID
- Password assignment
- Lock screen with password activation

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, or as required by law (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

We will generally keep your information for periods as recommended by law. Once the periods have expired, the information will be destroyed if it is no longer required for the reasons it was obtained. Our full retention schedule is available by contacting the office on 0141 578 0200, emailing us at mwhite@hillheadhousing.org or from our website: https://hillheadhousing.org/contact-us/

Your Rights

You have the right at any time to:

- ask for a copy of the information about you held by us in our records;
- require us to correct any inaccuracies in your information;
- in certain situations, make a request to us to delete your personal data;
- request we restrict processing your personal data;
- object to receiving any marketing communications from us, and;
- to be informed of any automated decisions made in relation to you.

Any questions relating to this notice and our privacy practices should be directed, in the first instance, to mwhite@hillheadhousing.org or by telephoning 0141 578 0200
Our Data Protection Officer is provided by RGDP LLP and can be contacted either via 0131 222 3239 or info@rgdp.co.uk

You also have the right to complain to the Information Commissioner's Office in relation to our use of your information. The Information Commissioner's contact details are noted below:

The Information Commissioner's Office – Scotland
Queen Elizabeth House
Sibbald Walk
Edinburgh
EH8 8FT

Telephone: 01303 123 1115
Email: scotland@ico.org.uk

The accuracy of your information is important to us - please help us keep our records updated by informing us of any changes to your email address and other contact details.

APPENDIX 2 – DATA SHARING AGREEMENT

Data Sharing Agreement

Between

Hillhead Housing Association 2000, registered as:

A Scottish Charity (Scottish Charity Number SC029908);
A registered society under the Co-operative and Community Benefit Societies Act 2014;
With the Financial Services Agency with Registered Number 2562RS;
With the Scottish Housing Regulator with Registration Number 326

and having their Registered Office at: **2 Meiklehill Road, Hillhead, Kirkintilloch, G66 2LA**

and

#*[Insert organisation name, a # [e.g. Company]* registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at #[*address]*] ("#**[Party 2]**")]") ***[Drafting note: amend from Party 2 to suitable defined term]***;

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

WHEREAS

(a) Data Controller and [*Insert name of party*] ("[Party 2]")intend that this data sharing agreement will form the basis of the data sharing arrangements between the parties (the "Agreement"); and

(b) The intention of the Parties is that they shall each be independent Data Controllers in respect of the Data that they process under this Agreement.

(c) Nothing in this Agreement shall alter, supersede, or in any other way affect the terms of #[***insert details of relationship/ contract with Party 2***]

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS

1.1 In construing this Agreement, capitalised words and expressions shall have the meaning set out opposite:

"Agreement" means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including the Schedule;

"Business Day" means any day which is not a Saturday, a Sunday or a bank or public holiday throughout Scotland;

"Data" means the information which contains Personal Data and Special Category Personal Data (both of which have the definition ascribed to them in Data Protection Law) described in Part 1;

"Data Controller" has the meaning set out in Data Protection Law;

"Disclosing Party" means the Party (being either #[Party1] or #[Party 2], as appropriate) disclosing Data (or on behalf of whom Data is disclosed to the Data Recipient);

"Data Protection Law" means Law relating to data protection, the processing of personal data and privacy from time to time, including:

(a) the Data Protection Act 2018;
(b) the General Data Protection Regulation (EU) 2016/679;
(c) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
(d) Any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union;

"Data Recipient" means the party (being either #[Party1] or #[Party 2], as appropriate) to whom Data is disclosed;

"Data Subject" means any identifiable individual to whom any Data relates: and the categories of data subjects within the scope of this Agreement are listed in Part 1;

"Data Subject Request" means a request of either party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the data or the activities of the parties contemplated by this Agreement;

"Disclosing Party" means the party (being either #[Party1] or #[Party 2], as appropriate) disclosing Data to the Data Recipient;

"Information Commissioner" means the UK Information Commissioner and any successor;

"Law" means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or other binding restriction, decision or guidance in force from time to time;

"Legal Basis" means in relation to either Party, the legal basis for sharing the Data as described in Clause **Error! Reference source not found.** and as set out in Part 2;

"Purpose" means the purpose referred to in Part 2;

"Representatives" means, as the context requires, the representative of #[Party1] and/or the representative of #[Party 2] as detailed in Part 4 of the Schedule. The same may be changed from time to time on notice in writing by the relevant Party to the other Party;

"Schedule" means the Schedule in 6 Parts annexed to this Agreement and a reference to a "Part" is to a Part of the Schedule; and

"Security Measures" has the meaning given to that term in Clause **Error! Reference source not found.**.

1.2 In this Agreement unless the context otherwise requires:

1.2.1 words and expressions defined in Data Protection Law shall have the same meanings in this Agreement so that, in the case of Data Protection Law, words and expressions shall be interpreted in accordance with:
(a) the General Data Protection Regulation (EU) 2016/679; and
(b) the UK Data Protection Act 2018;

1.2.2 more generally, references to statutory provisions include those statutory provisions as amended, replaced, re-enacted for the time being in force and shall include any bye-laws, statutory instruments, rules, regulations, orders, notices, codes of practice, directions, consents or permissions and guidelines (together with any conditions attached to the foregoing) made thereunder;

2 DATA SHARING

Purpose and Legal Basis

2.1 The Parties agree to share the Data for the Purpose in accordance with the provisions of Part 2 of the Schedule.

2.2 Save as provided for in this Agreement, the Parties agree not to use any Data disclosed in terms of this Agreement in a way that is incompatible with the Purpose.

2.3 Each Party shall ensure that it processes the Data fairly and lawfully in accordance with Data Protection Law and each Party as Disclosing Party warrants to the other Party in relation to any Data disclosed, that such disclosure is justified by a Legal Basis.

Parties Relationship

2.4 The Parties agree that the relationship between them is such that any processing of the Data shall be on a Data Controller to Data Controller basis. The Data Recipient agrees that:

2.4.1 it is a separate and independent Data Controller in respect of the Data that it processes under this Agreement, and that the Parties are not joint Data Controllers or Data Controllers in common;

2.4.2 it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);

2.4.3 it shall comply with its obligations under Part 6 of the Schedule;

2.4.4 it shall not transfer any of the Data outside the United Kingdom except to the extent agreed by the Disclosing Party;

2.4.5 Provided that where the Data has been transferred outside the United Kingdom, the Disclosing Party may require that the Data is transferred back to within the United Kingdom:

(a) on giving not less than 3 months' notice in writing to that effect; or

(b) at any time in the event of a change in Law which makes it unlawful for the Data to be processed in the jurisdiction outside the United Kingdom where it is being processed; and

2.4.6 it shall implement appropriate technical and organisational measures including the security measures set out in Part 5 of the Schedule (the "**Security Measures**"), so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data.

2.5 The Disclosing Party undertakes to notify in writing to the other as soon as practicable if an error is discovered in Data which has been provided to the Data Recipient, to ensure that the Data Recipient is then able to correct its records. This will happen whether the error is discovered through existing Data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to the Disclosing Party by the Data Subjects themselves).

Transferring Data

2.6 Subject to the Data Recipient's compliance with the terms of this Agreement, the Disclosing Party undertakes to endeavour to provide the Data to the Data Recipient on a non-exclusive basis in accordance with the transfer arrangements detailed in Part 3 of the Schedule.

3 BREACH NOTIFICATION

3.1 Each Party shall, promptly (and, in any event, no later than 12 hours after becoming aware of the breach or suspected breach) notify the other party in writing of any breach or suspected breach of any of that Party's obligations in terms of Clauses 1 and/or 2 and of

any other unauthorised or unlawful processing of any of the Data and any other loss or destruction of or damage to any of the Data. Such notification shall specify (at a minimum):

3.1.1 the nature of the personal data breach or suspected breach;

3.1.2 the date and time of occurrence;

3.1.3 the extent of the Data and Data Subjects affected or potentially affected, the likely consequences of any breach (in the case of a suspected breach, should it have occurred) for Data Subjects affected by it and any measures taken or proposed to be taken by the that party to contain the breach or suspected breach; and

3.1.4 any other information that the other Party shall require in order to discharge its responsibilities under Data Protection Law in relation to such breach or suspected breach.

3.2 The Party who has suffered the breach or suspected breach shall thereafter promptly, at the other Party's expense (i) provide the other Party with all such information as the other Party reasonably requests in connection with such breach or suspected breach; (ii) take such steps as the other Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on any of the Data Subjects and/or on the other Party; and (iii) otherwise cooperate with the other Party in investigating and dealing with such breach or suspected breach and its consequences.

3.3 The rights conferred under this Clause 3 are without prejudice to any other rights and remedies for breach of this Agreement whether in contract or otherwise in law.

4 DURATION, REVIEW AND AMENDMENT

4.1 This Agreement shall come into force immediately on being executed by all the Parties and continue for #[***insert termination: this will be when Parties cease sharing data in terms of contractual relationship with each other***], unless terminated earlier by the Disclosing Party in accordance with Clause 4.5.

4.2 This Agreement will be reviewed one year after it comes into force and every two years thereafter until termination or expiry in accordance with its terms.

4.3 In addition to these scheduled reviews and without prejudice to Clause 4.5, the Parties will also review this Agreement and the operational arrangements which give effect to it, if any of the following events takes place:

4.3.1 the terms of this Agreement have been breached in any material aspect, including any security breach or data loss in respect of Data which is subject to this Agreement; or

4.3.2 the Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.

4.4 Any amendments to this Agreement will only be effective when contained within a formal amendment document which is formally executed in writing by both Parties.

4.5 In the event that the Disclosing Party has any reason to believe that the Data Recipient is in breach of any of its obligations under this Agreement, the Disclosing Party may at its sole discretion:

4.5.1 suspend the sharing of Data until such time as the Disclosing Party is reasonably satisfied that the breach will not re-occur; and/or

4.5.2 terminate this Agreement immediately by written notice to the Data Recipient if the Data Recipient commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within five (5) Business Days of receiving written notice of the breach.

4.6 Where the Disclosing Party exercises its rights under Clause **Error! Reference source not found.**, it may request the return of the Data (in which case the Data Recipient shall, no later than fourteen (14) days after receipt of such a written request from the Disclosing Party, at the Disclosing Party's option, return or permanently erase/destroy all materials held by or under the control of the Data Recipient which contain or reflect the Data and shall not retain any copies, extracts or other reproductions of the Data either in whole or in part and shall confirm having done so to the other Party in writing), save that the Data Recipient will be permitted to retain one copy for the purpose of complying with, and for so

long as required by, any law or judicial or administrative process or for its legitimate internal compliance and/or record keeping requirements.

5 LIABILITY

5.1 Nothing in this Agreement limits or excludes the liability of either Party for:

5.1.1 death or personal injury resulting from its negligence; or

5.1.2 any damage or liability incurred as a result of fraud by its personnel; or

5.1.3 any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.

5.2 The Data Recipient indemnifies the Disclosing Party against any losses, costs, damages, awards of compensation, any monetary penalty notices or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred by the Disclosing Party, or awarded, levied or imposed against the other party, as a result of any breach by the Data Recipient of its obligations under this Agreement. Any such liability arising from the terms of this Clause 5.2 is limited to £# (# STERLING) in the aggregate for the duration of this Agreement.

5.3 Subject to Clauses **Error! Reference source not found.** and **Error! Reference source not found.** above:

5.3.1 each Party excludes all liability for breach of any conditions implied by law (including any conditions of accuracy, security, completeness, satisfactory quality, fitness for purpose, freedom from viruses, worms, trojans or other hostile computer programs, non-infringement of proprietary rights and the use of reasonable care and skill) which but for this Agreement might have effect in relation to the Data;

5.3.2 neither Party shall in any circumstances be liable to the other party for any actions, claims, demands, liabilities, damages, losses, costs, charges and expenses that the other party may suffer or incur in connection with, or arising (directly or indirectly) from, any use of or reliance on the Data provided to them by the other Party; and

5.3.3 use of the Data by both Parties is entirely at their own risk and each party shall make its own decisions based on the Data, notwithstanding that this Clause shall not prevent one party from offering clarification and guidance to the other party as to appropriate interpretation of the Data.

6 DISPUTE RESOLUTION

6.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.

6.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to the following individuals in Part 4 of the Schedule identified as escalation points who will endeavour in good faith to resolve the issue.

6.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause **Error! Reference source not found.**, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.

6.4 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 6.1 to 6.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause **Error! Reference source not found.**.

6.5 The provisions of Clauses 6.1 to 6.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

7 NOTICES

7.1 Any Notices to be provided in terms of this Agreement must be provided in writing and addressed to the relevant Party in accordance with the contact details noted in Part 4 of the Schedule, and will be deemed to have been received (i) if delivered personally, on the day of delivery; (ii) if sent by first class post or other next working day delivery, the second day after posting; (iii) if by courier, the date and time the courier's delivery receipt if signed; or (iv) if by fax, the date and time of the fax receipt.

8 GOVERNING LAW

This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) (a **"Dispute"**) shall, in all respects, be governed by and construed in accordance with the law of Scotland. Subject to Clause 6, the Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

IN WITNESS WHEREOF these presents consisting of this and the preceding 6 pages together with the Schedule in 6 parts hereto are executed by the Parties hereto as follows:

On behalf of PARTY1

at

on

by

Print Full Name Director/Secretary/Authorised Signatory

before this witness

Print Full Name Witness

Address

On behalf of #[Party 2]

at

on

by

Print Full Name Authorised Signatory

before this witness

Print Full Name Witness

Address

_____

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN #[PARTY1] AND #[PARTY 2]

SCHEDULE PART 1 – DATA

DATA SUBJECTS

For the purposes of this Agreement, Data Subjects are all living persons about whom information is transferred between the Parties.

SCHEDULE PART 2: PURPOSE AND LEGAL BASIS FOR PROCESSING

Purpose

The Parties are exchanging Data to allow

Legal Basis

SCHEDULE PART 3 - DATA TRANSFER RULES

Information exchange can only work properly in practice if it is provided in a format which the Data Recipient can utilise. It is also important that the Data is disclosed in a manner which ensures that no unauthorised reading, copying, altering or deleting of personal data occurs during electronic transmission or transportation of the Data. The Parties therefore agree that to the extent that data is physically transported, the following media are used:

- Face to face
- Secure email
- Courier
- Encrypted removable media

The data is encrypted, with the following procedure(s):

SCHEDULE PART 4 – REPRESENTATIVES

Contact Details

#[Party 1]

Name: #

Job Title: #

Address: #

E-mail: #

Telephone Number: #

#[Party 2]

Name: #

Job Title: #

Address: #

E-mail: #

Telephone Number: #

SCHEDULE PART 5 – SECURITY MEASURES

1 The Parties shall each implement an organisational information security policy.

2 Physical Security

2.1 Any use of data processing systems by unauthorised persons must be prevented by means of appropriate technical (keyword / password protection) and organisational (user master record) access controls regarding user identification and authentication. Any hacking into the systems by unauthorised persons must be prevented. Specifically, the following technical and organisational measures are in place:
The unauthorised use of IT systems is prevented by:

- User ID
- Password assignment
- Lock screen with password activation
- Each authorised user has a private password known only to themselves
- Regular prompts for password amendments

The following additional measures are taken to ensure the security of any Data:

3 Disposal of Assets

3.1 Where information supplied by a Party no longer requires to be retained, any devices containing Personal Data must be physically destroyed or the information must be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

4 Malicious software and viruses

Each Party must ensure that:

4.1.1 PCs used in supporting the service are supplied with anti-virus software and anti-virus and security updates are promptly applied.

4.1.2 All files received by one Party from the other are scanned to ensure that no viruses are passed.

4.1.3 The Parties must notify each other of any virus infections that could affect their systems on Data transfer.

APPENDIX 3 – DATA PROTECTION ADDENDUM

Data Processor Contract Addendum

between

Hillhead Housing Association 2000, registered as:

A Scottish Charity (Scottish Charity Number SC029908);
A registered society under the Co-operative and Community Benefit Societies Act 2014;
With the Financial Services Agency with Registered Number 2562RS;
With the Scottish Housing Regulator with Registration Number 326

and having their Registered Office at: **2 Meiklehill Road, Hillhead, Kirkintilloch, G66 2LA**

and

#*[Insert organisation name, a # [e.g. Company]* registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at #[*address]*] ("#**[Party 2]**")]") ***[Drafting note: amend from Party 2 to suitable defined term]***;

WHEREAS the Controller processes Personal Data in connection with its business activities; and whereas the Controller has engaged the services of the Processor to process Personal Data on its behalf, the parties do hereby agree as follows:-

1. Definitions

1.1 The terms **"process/processing", "data subject", "data processor", "data controller", "personal data", "personal data breach"**, and **"data protection impact assessment"** shall have the same meaning as described in Data Protection Laws;

1.2 "**Addendum**" means this Data Processor Contract Addendum;

1.3 "**Authorised Sub-processors**" means (a) those Sub-processors (if any) set out in Schedule 2 (*Authorised Sub-processors*); and (b) any additional Sub-processors consented to in writing by [INSERT NAME OF CUSTOMER] in accordance with section 5.1;

1.4 "**Data Protection Laws**" means, in relation to any Personal Data which is Processed in the performance of the Main Agreement, the General Data Protection Regulation (EU) 2016/679 ("GDPR"); the UK Data Protection Act 2018; the EU Directive 2002/58/EC on privacy and electronic communications, as transposed into domestic legislation of each Member State; and any applicable decisions, guidelines, guidance notes and codes of practice issued from time to time by courts, supervisory authorities and other applicable government authorities; in each case together with all laws implementing, replacing, amending or supplementing the same and any other applicable data protection or privacy laws;

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

1.6 "**Personal Data**" means the data described in Schedule 1 (*Details of Processing of Personal Data*) and any other personal data processed by the Supplier on behalf of [INSERT NAME OF CUSTOMER] pursuant to or in connection with the Main Agreement;

1.7 "**Main Agreement**" means the services agreement into which this Addendum is incorporated;

1.8 "**Services**" means the services described in the Main Agreement;

1.9 “**Standard Contractual Clauses**” means the standard contractual clauses for the transfer of personal data to processors established in third countries, as approved by the European Commission in Decision 2010/87/EU, or any set of clauses approved by the European Commission which amends, replaces or supersedes these;

1.10 “**Sub-processor**” means any data processor (including any affiliate of the Supplier) appointed by the Supplier to process personal data on behalf of [INSERT NAME OF CUSTOMER];

1.11 “**Supervisory Authority**” means (a) an independent public authority which is established by a Member State pursuant to Article 51 GDPR; and (b) any similar regulatory authority responsible for the enforcement of Data Protection Laws;

1.12 **“Supplier”** means the Supplier under the Main Agreement.

2. Processing of Personal Data

2.1 The parties agree that [INSERT NAME OF CUSTOMER] is a data controller and that the Supplier is a data processor for the purposes of processing Personal Data.

2.2 Each party shall at all times in relation to processing connected with the Main Agreement comply with Data Protection Laws.

2.3 The Supplier shall only process the types of Personal Data relating to the categories of data subjects for the purposes of the Main Agreement and for the specific purposes in each case as set out in Schedule 1 (Details of Processing of Personal Data) to this Addendum and shall not process, transfer, modify, amend or alter the Personal Data or disclose or permit the disclosure of the Personal Data to any third party other than in accordance with [INSERT NAME OF CUSTOMER] documented instructions (whether in the Main Agreement or otherwise) unless processing is required by applicable law to which the Supplier is subject, in which case the Supplier shall to the extent permitted by such law inform [INSERT NAME OF CUSTOMER] of that legal requirement before processing that Personal Data.

2.4 The Supplier shall immediately inform [INSERT NAME OF CUSTOMER], if in its opinion, an instruction pursuant to the Main Agreement or this Addendum infringes Data Protection Laws.

2.5 [INSERT NAME OF CUSTOMER] warrants to and undertakes with the Supplier that all data subjects of the Personal Data have been or will be provided with appropriate privacy notices and information to establish and maintain for the relevant term the necessary legal grounds under Data Protection Laws for transferring the Personal Data to the Supplier to enable the Supplier to process the Personal Data in accordance with this Addendum and the Main Agreement.

3. Processor Personnel

3.1 The Supplier shall treat all Personal Data as strictly confidential and shall inform all its employees, agents, contractors and/or Authorised Sub-processors engaged in processing the Personal Data of the confidential nature of such Personal Data.

3.2 The Supplier shall take reasonable steps to ensure the reliability of any employee, agent, contractor and/or Authorised Sub-processor who may have access to the Personal Data, ensuring in each case that access is limited to those persons or parties who need to access the relevant Personal Data, as necessary for the purposes set out in section 2.1 above in the context of that person's or party's duties to the Supplier.

3.3 The Supplier shall ensure that all such persons or parties involved in the processing of Personal Data are subject to:

3.3.1 confidentiality undertakings or are under an appropriate statutory obligation of confidentiality; and

3.3.2 user authentication processes when accessing the Personal Data.

4. Security

4.1 The Supplier shall implement appropriate technical and organisational measures to ensure a level of security of the Personal Data appropriate to the risks that are presented by the processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

5. Sub-processing

5.1 Subject to section 5.4, the Supplier shall not engage any Sub-processor to process Personal Data other than with the prior specific or general written authorisation of [INSERT NAME OF CUSTOMER].

5.2 In the case of general written authorisation, the Supplier shall inform [INSERT NAME OF CUSTOMER] of any intended changes concerning the addition or replacement of other processors, thereby giving [INSERT NAME OF CUSTOMER] the opportunity to object to such changes.

5.3 With respect to each Sub-processor, the Supplier shall:

5.3.1 carry out adequate due diligence on each Sub-processor to ensure that it is capable of providing the level of protection for the Personal Data as is required by this Addendum including without limitation sufficient guarantees to implement appropriate technical and organisational measures in such a manner that Processing will meet the requirements of Data Protection Laws and this Addendum;

5.3.2 include terms in the contract between the Supplier and each Sub-processor which are the same as those set out in this Addendum, and shall supervise compliance thereof;

5.3.3 insofar as that contract involves the transfer of Personal Data outside of the EEA, incorporate the Standard Contractual Clauses or such other mechanism as directed by [INSERT NAME OF CUSTOMER] into the contract between the Supplier and each Sub-processor to ensure the adequate protection of the transferred Personal Data, or such other arrangement as [INSERT NAME OF CUSTOMER] may approve as providing an adequate protection in respect of the processing of Personal Data in such third country(ies); and

5.3.4 remain fully liable to [INSERT NAME OF CUSTOMER] for any failure by each Sub-processor to fulfil its obligations in relation to the Processing of any Personal Data.

5.4 As at the date of the Main Agreement or (if later) implementation of this Addendum, [INSERT NAME OF CUSTOMER] hereby authorises the Supplier to engage those Sub-processors set out in Schedule 2 (*Authorised Sub-processors*).

6. Data Subject Rights

6.1 The Supplier shall without undue delay, and in any case within two (2) working days, notify [INSERT NAME OF CUSTOMER] if it receives a request from a data subject under any Data Protection Laws in respect of Personal Data, including requests by a data subject to exercise rights in chapter 3 of GDPR, and shall provide full details of that request.

6.2 The Supplier shall co-operate as reasonably requested by [INSERT NAME OF CUSTOMER] to enable [INSERT NAME OF CUSTOMER] to comply with any exercise of rights by a data subject under any Data Protection Laws in respect of Personal Data and to comply with any assessment, enquiry, notice or investigation under any Data Protection Laws in respect of Personal Data or the Main Agreement, which shall include:

6.2.1 the provision of all information reasonably requested by [INSERT NAME OF CUSTOMER] within any reasonable timescale specified by [INSERT NAME OF CUSTOMER] in each case, including full details and copies of the complaint, communication or request and any Personal Data it holds in relation to a data subject;

6.2.2 where applicable, providing such assistance as is reasonably requested by [INSERT NAME OF CUSTOMER] to enable [INSERT NAME OF CUSTOMER] to comply with the relevant request within the timescales prescribed by Data Protection Laws; and

6.2.3 implementing any additional technical and organisational measures as may be reasonably required by [INSERT NAME OF CUSTOMER] to allow [INSERT NAME OF CUSTOMER] to respond effectively to relevant complaints, communications or requests.

7. Personal Data Breach Management

7.1 In the case of a personal data breach, the Supplier shall without undue delay notify the personal data breach to [INSERT NAME OF CUSTOMER] providing [INSERT NAME OF CUSTOMER] with sufficient information which allows [INSERT NAME OF CUSTOMER] to meet any obligations to report a personal data breach under Data Protection Laws. Such notification shall as a minimum:

7.1.1 describe the nature of the personal data breach, the categories and numbers of data subjects concerned, and the categories and numbers of Personal Data records concerned;

7.1.2 communicate the name and contact details of the Supplier's data protection officer or other relevant contact from whom more information may be obtained;

7.1.3 describe the likely consequences of the personal data breach; and

7.1.4 describe the measures taken or proposed to be taken to address the data breach, including, where appropriate, measures to mitigate its possible adverse effects.

7.2 The Supplier shall fully co-operate with [INSERT NAME OF CUSTOMER] and take such reasonable steps as are directed by [INSERT NAME OF CUSTOMER] to assist in the investigation, mitigation and remediation of each personal data breach, in order to enable [INSERT NAME OF CUSTOMER] to *(i)* perform a thorough investigation into the personal data breach, *(ii)* formulate a correct response and to take suitable further steps in respect of the personal data breach in order to meet any requirement under Data Protection Laws.

7.3 The parties agree to coordinate and cooperate in good faith on developing the content of any related public statements or any required notices for the affected persons. The Supplier shall not inform any third party without first obtaining [INSERT NAME OF CUSTOMER] prior written consent, unless notification is required by law to which the Supplier is subject, in which case the Supplier shall to the extent permitted by such law inform [INSERT NAME OF CUSTOMER] of that legal requirement, provide a copy of the proposed notification and consider any comments made by [INSERT NAME OF CUSTOMER] before notifying the personal data breach.

8. Data protection impact assessments and consultation

8.1 The Supplier shall, at [INSERT NAME OF CUSTOMER] request, provide reasonable assistance to [INSERT NAME OF CUSTOMER] with any data protection impact assessments and any consultations with any Supervisory Authority of [INSERT NAME OF CUSTOMER] as may be required in relation to the processing of Personal Data by the Supplier on behalf of [INSERT NAME OF CUSTOMER].

9. Deletion or return of controller personal data

9.1 The Supplier shall promptly and in any event within 90 (ninety) calendar days of the earlier of: *(i)* cessation of processing of Personal Data by the Supplier; or *(ii)* termination of the Main Agreement, at the choice of [INSERT NAME OF CUSTOMER] either return all Personal Data to [INSERT NAME OF CUSTOMER] or securely dispose of Personal Data (and thereafter promptly delete all existing copies of it) except to the extent that any applicable law requires the Supplier to store such Personal Data.

10. Audit rights

10.1 The Supplier shall make available to [INSERT NAME OF CUSTOMER] on request all information necessary to demonstrate compliance with this Addendum and Data Protection Laws and allow for and contribute to audits, including inspections by [INSERT NAME OF CUSTOMER] or another auditor mandated by [INSERT NAME OF CUSTOMER] of any premises where the processing of Personal Data takes place.

10.2 The Supplier shall permit [INSERT NAME OF CUSTOMER] or another auditor mandated by [INSERT NAME OF CUSTOMER] during normal working hours and on reasonable prior notice to inspect, audit and copy any relevant records, processes and systems in order that [INSERT NAME OF CUSTOMER] may satisfy itself that the provisions of Data Protection Laws and this Addendum are being complied with.

10.3 The Supplier shall provide full co-operation to [INSERT NAME OF CUSTOMER] in respect of any such audit and shall at the request of [INSERT NAME OF CUSTOMER], provide [INSERT NAME OF CUSTOMER] with evidence of compliance with its obligations under this Addendum and Data Protection Laws.

11. International transfers of controller personal data

11.1 The Supplier shall not (permanently or temporarily) process the Personal Data nor permit any Authorised Sub-processor to (permanently or temporarily) process the Personal Data in a country outside of the EEA without an adequate level of protection, other than in respect of those recipients in such countries listed in Schedule 3 (*Authorised Transfers of Personal Data*), unless authorised in writing by [INSERT NAME OF CUSTOMER] in advance.

11.2 When requested by [INSERT NAME OF CUSTOMER], the Supplier shall promptly enter into (or procure that any relevant Sub-processor of the Supplier enters into) an agreement with [INSERT NAME OF CUSTOMER] on Standard Contractual Clauses and/or such variation as Data Protection Laws might require, in respect of any processing of Personal Data in a country outside of the EEA without an adequate level of protection.

12. Liability

12.1 The disclaimers and limitations of liability set out under the Main Agreement shall apply also to this Addendum.

13. Costs

13.1 [INSERT NAME OF CUSTOMER] shall pay any reasonable costs and expenses incurred by the Supplier in meeting [INSERT NAME OF CUSTOMER] requests made under this Addendum.

14. Miscellaneous

14.1 Any obligation imposed on the Supplier under this Addendum in relation to the processing of Personal Data shall survive any termination or expiration of the Main Agreement.

14.2 With regard to the subject matter of this Addendum, in the event of any conflict or inconsistency between any provision of the Main Agreement and any provision of this Addendum, the provision of this Addendum shall prevail. In the event of any conflict or inconsistency between the Main Agreement or this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail.

15. Signatories

This Agreement is signed on behalf of each of the parties by its duly authorised representative as follows:-

_____	_____
SIGNATURE	[CONTROLLER]
_____	_____
SIGNATURE	[PROCESSOR]

SCHEDULE 1: Details of Processing of Personal Data

This Schedule 1 includes certain details of the processing of Personal Data as required by Article 28(3) GDPR.

Subject matter and duration of the processing of Personal Data
[ENTER DETAILS]
The nature and purpose of the processing of Personal Data
[ENTER DETAILS]
The types of Personal Data to be processed
[ENTER DETAILS
The categories of data subject to whom the Personal Data relates
[ENTER DETAILS]

SCHEDULE 2: Authorised sub-processors

[ENTER DETAILS] ***(if relevant to this agreement)***

SCHEDULE 3: Authorised transfers of controller personal data

[ENTER DETAILS] ***(if relevant to this agreement)***