

***Paragon Housing Association Limited***

**POLICY:** Data Protection, GDPR & Access to Information

**POLICY AREA:** GOVERNANCE

**DATE APPROVED:** 30<sup>th</sup> May 2018

**DATE NEXT REVIEW:** May 2021

## **Contents**

1. Introduction	p 1
2. Legislation	p 1
3. Data	p 2
4. Processing of Personal Data	p 3
5. Data Sharing	p 5
6. Data Storage and Security	p 6
7. Breaches	p 7
8. Data Protection Officer	p 8
9. Data Subject Rights	p 9
10. Privacy Impact Assessments	p 11
11. Archiving, Retention and Destruction of Data	p11

## **1. Introduction**

Paragon Housing Association] (hereinafter the “Association”) is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals. The Association’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.

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

This Policy sets out the Association’s duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

Appendix 1 hereto details the Association’s related policies.

## **2. Legislation**

It is a legal requirement that the Association process data correctly; the Association 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 (EU) 2016/679 (“the GDPR”);

- (b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- (c) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or 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

### **3. Data**

3.1 The Association holds a variety of Data 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 the Association is detailed within the Fair Processing Notice at Appendix 2 hereto and the Data Protection Addendum of the Terms of and Conditions of Employment which has been provided to all employees.

3.1.1 “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 the Association.

3.1.2 The Association 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 The Association 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 clause 4.4 hereof);
- Processing is necessary for the performance of a contract between the Association and the data subject or for entering into a contract with the data subject;
- Processing is necessary for the Association'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 the Association's official authority; or
- Processing is necessary for the purposes of legitimate interests.

### **4.2 Fair Processing Notice**

4.2.1 The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal data is held by the Association. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them.

4.2.2 The Fair Processing Notice at Appendix 2 sets out the Personal Data processed by the Association and the basis for that Processing. This document is provided to all of the Association's customers at the outset of processing their data

### **4.3 Employees**

4.3.1 Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the Association. Details of the data held and processing of that data is contained within the Employee Fair Processing Notice which is provided to Employees at the same time as their Contract of Employment.

4.3.2 A copy of any employee's Personal Data held by the Association is available upon written request by that employee from the Association's Director.

### **4.4 Consent**

Consent as a ground of processing will require to be used from time to time by the Association when processing Personal Data. It should be used by the Association where no other alternative ground for processing is available. In the event that the Association requires to obtain consent to process a data subject's Personal Data, it shall 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 the Association 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 the Association processes Special Category Personal Data or Sensitive Personal Data, the Association 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**

5.1 The Association shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with the Association's relevant policies and procedures. In order that the Association can monitor compliance by these third parties with Data Protection laws, the Association will require the third party organisations to enter in to an Agreement with the Association governing the processing of data, security measures to be implemented and responsibility for breaches.

### **5.2 Data Sharing**

5.2.1 Personal data is from time to time shared amongst the Association and third parties who require to process personal data that the Association process as well. Both the Association and the third party will be processing that data in their individual capacities as data controllers.

5.2.2 Where the Association shares in the processing of personal data with a third party organisation (e.g. for processing of the employees' pension), it shall require the third party organisation to enter in to a Data Sharing Agreement with the Association in accordance with the terms of the model Data Sharing Agreement set out in Appendix 3 to this Policy.

### **5.3 Data Processors**

A data processor is a third party entity that processes personal data on behalf of the Association, and are frequently engaged if certain of the Association's work is outsourced (e.g. payroll, maintenance and repair works).

- 5.3.1 A data processor must comply with Data Protection laws. The Association's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the Association if a data breach is suffered.
- 5.3.2 If a data processor wishes to sub-contact their processing, prior written consent of the Association 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.
- 5.3.3 Where the Association contracts with a third party to process personal data held by the Association, it shall require the third party to enter in to a Data Protection Addendum with the Association in accordance with the terms of the model Data Protection Addendum set out in Appendix 4 to this Policy.

## **6. Data Storage and Security**

All Personal Data held by the Association 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 requires to be retained on a physical file then the

employee should ensure that it is affixed to the file which is then stored in accordance with the Association'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 the Association's data processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be 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 drives and servers.

## **7. Breaches**

7.1 A data breach can occur at any point when handling Personal Data and the Association 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 who are subject of the breach require to be reported externally in accordance with Clause 7.3 hereof.

### **7.2 Internal Reporting**

The Association 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 (6) hours after it has occurred, the DPO must be notified in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- The Association 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 clause 7;
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements

### **7.3 Reporting to the ICO**

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("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")**

8.1. A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws. The Association has elected to appoint a Data Protection Officer whose details are noted on the Association's website and contained within the Fair Processing Notice at Appendix 3 hereto.

8.2 The DPO will be responsible for:

- 8.2.1 monitoring the Association's compliance with Data Protection laws and this Policy;
- 8.2.2 co-operating with and serving as the Association's contact for discussions with the ICO
- 8.2.3 reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

## **9. Data Subject Rights**

9.1 Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by the Association, whether in written or electronic form.

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to the Association's processing of their data. These rights are notified to the Association's tenants and other customers in the Association's Fair Processing Notice.

### **9.3 Subject Access Requests**

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

9.3.1 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.

9.3.2 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

9.3.3 where the Association 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.

#### **9.4 The Right to be Forgotten**

9.4.1 A data subject can exercise their right to be forgotten by submitting a request in writing to the Association seeking that the Association erase the data subject's Personal Data in its entirety.

9.4.2 Each request received by the Association 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 clause 9.4 and will respond in writing to the request.

#### **9.5 The Right to Restrict or Object to Processing**

9.5.1 A data subject may request that the Association restrict its processing of the data subject's Personal Data, or object to the processing of that data.

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

9.5.2 Each request received by the Association 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 clause 9.5 and will respond in writing to the request.

## **10. Privacy Impact Assessments (“PIAs”)**

10.1 These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of data subjects.

10.2 The Association shall:

10.2.1 Carry out a PIA 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 IT system for storing and accessing Personal Data; and

10.2.2 In carrying out a PIA, 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

10.3 The Association will require to consult the ICO in the event that a PIA identifies a high level of risk which cannot be reduced. The Data Protection Officer (“DPO”) will be responsible for such reporting, and where a high level of risk is identified by those carrying out the PIA they require to notify the DPO within five (5) working days.

## **11. Archiving, Retention and Destruction of Data**

The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. The Association shall ensure that all Personal data is archived and destroyed in accordance with the periods specified within the table at Appendix 5 hereto.

## **List of Appendices**

1. Table of Duration of Retention of certain Data
2. Fair Processing Notice
3. Personal Data Map
4. Employee Fair Processing Notice
5. Employment Contract Data Protection Wording
6. Data Protection Addendum
7. Data Sharing Agreement



## Appendix 1 Data Retention Periods

The table below sets out retention periods for Personal Data held and processed by the Association. It is intended to be used as a guide only. The Association recognises that not all Personal Data can be processed and retained for the same duration, and retention will depend on the individual circumstances relative to the Data Subject whose Personal Data is stored.

Type of record	Suggested retention time
Membership records	Permanently
Personal files including training records and notes of disciplinary and grievance hearings	6 years to cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of the redundancy
Application forms, interview notes	Minimum 6 months to a year from date of interviews. Successful applicants documents should be transferred to personal file.
Documents proving the right to work in the UK	2 years after employment ceases.
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.
Income tax, NI returns, correspondence with tax office	At least 6 years after the end of the tax year they relate to
Pensions & retirement benefits schemes – notifiable events, e.g. relating to incapacity	6 years from end of the scheme year in which the event took place

Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	6 years after the end of the tax year to which they relate
Parental Leave	18 years
Statutory Sick Pay records, calculations, certificates, self-certificates	6 years
Wages/salary records, expenses, bonuses	6 years
Records relating to working time	2 years from the date they were made
Accident books and records and reports of accidents	Permanently
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently
Health records	During employment and 3 years thereafter if reason for termination of employment is connected to health
Board Members Documents	Permanently
Documents relation to successful tenders	6 years after end of contract
Documents relating to unsuccessful form of tender	6 years after notification
Applicants for accommodation	Current application for duration of live application and 3 years for cancelled applications from date of cancellation
Housing Benefits Notifications	Duration of Tenancy & 2 years after tenancy end
Tenancy files	Duration of Tenancy
Former tenants' files (key info)	6 years from Tenancy end date.
Owner Files	Duration of factoring
Former Owner Files	6 years from factoring end date



Third Party documents re care plans	Duration of Tenancy
Records re offenders. Ex-offenders (sex offender register)	Duration of Tenancy
Lease documents	5 years after lease termination
ASB case files	5 years/end of legal action
Board meetings/residents' meetings documentation	5 years
Minute of factoring meetings	Duration of appointment



# **Paragon Housing Association GDPR Fair Processing 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?**

Paragon Housing Association a Scottish Charity (Scottish Charity Number SC036262), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2521R(s) and having their Registered Office at Invergrange House, Station Rd, Grangemouth FK3 8DG (“**we**” or “**us**”) take the issue of security and data protection very seriously and strictly adhere to guidelines published in the [Data Protection Act of 1998] and the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25th May 2018, together with any domestic laws subsequently enacted.

We are notified as a Data Controller with the Office of the Information Commissioner under registration number Z5624595 and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is Pamela Milne, Finance and Investment Manager.

Contact [pmilne@paragonha.org.uk](mailto:pmilne@paragonha.org.uk) Invergrange House, Station Rd, Grangemouth FK3 8DG

Any questions relating to this notice and our privacy practices should be sent to our Data Protection Officer set out above.

## **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 in to 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 collect the following information about you:

- name;
- address;
- correspondence address;
- telephone number;
- e-mail address;
- National Insurance Number;
- date of birth;
- next of kin;
- gender;
- household composition;
- employment details;
- income;
- housing benefit / universal credit details;
- title deeds;
- complaints;
- anti-social behaviour;
- behaviour warnings;
- references;
- photo identification;
- arrears information;

- criminal activity;
- race;
- ethnic origin;
- disability;
- medical information;
- any permission requests;
- payment details;
- survey information.

We 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;
- 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;
- to enable us to supply you with the services and information which you have requested;
- to enable us to respond to your repair request, housing application and complaints made;

- to analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;
- to contact you in order to send you details of any changes to our or supplies which may affect you;
- for all other purposes consistent with the proper performance of our operations and business; and
- to 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 merged 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 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);
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department of Work & Pensions;
- 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 we are recovering debt from current or former tenancy arrears, including recharges;
- If we are processing an insurance claim, your information will be shared with our insurance company;
- If requested by an emergency service.

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. We may transfer your information outside the UK and/or EEA.

If you are an owner and we factor your property and you are living out with the UK, invoices and other relevant information will be emailed to your specified email address.

Where information is transferred outside the UK or EEA we ensure that there are adequate safeguards in place to protect your information in accordance with this notice, including the following:

Password protected file sent by email.

### **Security**

When you give us information we take steps to make sure that your personal information is kept secure and safe.

We have taken the following steps:

- Our systems are password protected;
- Patch updates are applied to our servers;
- We regularly review our system access rights;
- Paper files are locked away;
- We restrict access only to relevant personnel;
- You will be asked to confirm your identity by answering questions or provide a signed mandate before we release information regarding your tenancy.

### **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 the following minimum periods:

- Current Tenancies – Duration of tenancy;
- Former Tenancies – 6 years from tenancy end date;
- Current Factored Owners - Duration of factoring;
- Former Factored Owners - 6 years from factoring end date;
- Current Applications – Duration of Application / Tenancy;
- Former Applications – 3 years from date of cancelled application;
- Current Members - Duration of membership;
- Former Members - Permanent record

after which this will be destroyed if it is no longer required for the reasons it was obtained.

### **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;
- make a request to us to delete what personal data of your we hold; and



- object to receiving any marketing communications from us.

If you would like to exercise any of your rights above please contact us at [enquires@paragonha.org.uk](mailto:enquires@paragonha.org.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

45 Melville Street, Edinburgh, EH3 7HL

Telephone: 0131 244 9001

Email: [Scotland@ico.org.uk](mailto: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 3 PERSONAL DATA MAP**

**Please refer to excel attachments**



## Appendix 4 Paragon Housing Association

---

### Employee Fair Processing Notice

(How we use employee 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.

1. Paragon Housing Association (“we” or “us”) is committed to a policy of protecting the rights of individuals with respect to the processing of their personal data and adhere to guidelines published in the [Data Protection Act of 1998] and the General Data Protection Regulation (EU) 2016/679 which is applicable from the 25th May 2018, together with any domestic laws subsequently enacted. We collect and use personal data for a variety of reasons.

We are notified as a Data Controller with the Office of the Information Commissioner under registration number Z5624595 and we are the data controller of any personal data that you provide to us.

Our Data Protection Officer is Pamela Milne, Finance and Investment Manager

Contact [pmilne@paragonha.org.uk](mailto:pmilne@paragonha.org.uk) Invergrange House, Station Rd, Grangemouth FK3 8DG

Any questions relating to this notice and our privacy practices should be sent to our DPO

2. We collect the following information from you through a variety of resources (i) directly from you; or (ii) third parties (including Employment Agencies, pensions service): We will ask for your explicit consent to collect sensitive personal data.

- (a) Name
- (b) Date of Birth
- (c) Address
- (d) Telephone Number
- (e) E-mail address

- (f) NI number
- (g) Personal characteristics such as gender and ethnic group
- (h) Qualifications
- (i) Absence information
- (j) Marital status
- (k) Medical history
- (l) Next of Kin

We collect and use the above information and personal data for:

- a. Administration of contracts of employment
  - b. Payment of salaries
  - c. Recruitment and selection
  - d. Pensions and associated benefits, appraisal, training and development
  - e. Membership of professional bodies
  - f. Providing information to the Scottish Housing Regulator
  - g. Reporting to Paragon Management Committee
  - h. Audit purposes
  - i. Insurance
3. We may disclose to and share information about you with third parties for the purposes set out in this notice, or for purposes approved by you, including the following:
- To process your monthly salary payments;
  - To allow your pension provider to process pensions information and handle your pension;
  - To allow your electronic payslips to be produced and issued to you;
  - Audit purposes
  - To provide personal and company insurance
  - If we enter into a joint venture with or is sold to or merged with another business entity, your information may be disclosed to our new business partners or owners.
4. Your information will only be stored within the UK and EEA
5. When you give us information we take steps to make sure that your personal information is kept secure and safe. Please refer to Paragon Data Protection Policy

6. 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.

Data retention guidelines on the information we hold is provided in our Data Protection Policy within the staff handbook.

7. You have the right at any time to:

- Ask for a copy of the information about you held by us in our records; and
- Require us to correct any inaccuracies in your information

8. If you would like to find out more about how we use your personal data or want to see a copy of information about you that we hold or wish to exercise any of your above rights, please contact our DPO

You have the right to complain to the Information Commissioner's Office in relation to our use of your information.

The accuracy of your information is important to us – please help us keep our records updated by informing us of any changes to your personal and contact details.



## **Appendix 5 Employment Contract – Data Protection Wording**

### **Employment Contract Amendment**

We hold information about you on your personal file. You are entitled to access this file and to other information that we hold about you, subject to certain restrictions imposed by law. The Fair Processing Notice annexed to this amendment to the Terms & Conditions of Employment (a duplicate copy of which we have provided to you) confirms what personal information we hold which we have obtained from you or third parties. Our Data Protection Policy contains further details regarding Data Protection matters, and the handling of personal data. By signing this amendment to the Terms & Conditions of Employment you confirm that you have read and understood our Data Protection Policy and will comply with the terms of that Policy.

We may also require to process sensitive personal data of yours. Any sensitive personal data we process to comply with our obligations as your employers and/ or your vital interests is outlined within the Fair Processing Notice annexed hereto. We will seek to obtain your consent to process any additional sensitive personal data of yours that we wish to process.

I ..... agree to the above amendment to my Terms and Conditions of Employment

Signed.....

Date.....

I agree / disagree to Paragon holding additional sensitive personal information, specifically Personal characteristics such as gender and ethnic group, marital status and medical history.

Please delete as appropriate

Signed.....

Date.....





## Appendix 6 DATA PROTECTION ADDENDUM

between

**Paragon Housing Association** a Scottish Charity (Scottish Charity Number SC036262), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2521R(s) and having their Registered Office at Invergrange House, Station Rd, Grangemouth FK3 8DG (the "Association");

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]* (the "Processor")

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

### WHEREAS

- (a) The Association and the Processor have entered in to an agreement/ contract to *#[insert detail]* (hereinafter the "Principal Agreement"/"Principal Contract");
- (b) This Data Protection Addendum forms part of the Principal Agreement/Principal Contract (\*delete as appropriate); and
- (c) In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

### 1. Definitions

- 1.1 The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement/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 **"Applicable Laws"** means (a) European Union or Member State laws with respect to any Company Personal Data in respect of which any Company Group Member is subject to EU Data Protection Laws; and (b) any other applicable law with respect to any Association Personal Data in respect of which any Company Group Member is subject to any other Data Protection Laws;

- 1.1.2 **"Association Personal Data"** means any Personal Data Processed by a Contracted Processor on behalf of the Association pursuant to or in connection with the Principal Agreement/Contract;
- 1.1.3 **"Contracted Processor"** means Processor or a Sub processor;
- 1.1.4 **"Data Protection Laws"** means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;
- 1.1.5 **"EEA"** means the European Economic Area;
- 1.1.6 **"EU Data Protection Laws"** means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR;
- 1.1.7 **"GDPR"** means EU General Data Protection Regulation 2016/679;
- 1.1.8 **"Restricted Transfer"** means:
  - 1.1.8.1 *a transfer of Association Personal Data from the Association to a Contracted Processor; or*
  - 1.1.8.2 *an onward transfer of Association Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,*in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);
- 1.1.9 **"Services"** means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Association pursuant to the Principal Agreement/ Contract;
- 1.1.10 **"Sub processor"** means any person (including any third party and any , but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor which is engaged in the Processing of Personal Data on behalf of the Association in connection with the Principal Agreement/Contract; and
- 1.2 The terms, **"Commission"**, **"Controller"**, **"Data Subject"**, **"Member State"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processing"** and **"Supervisory Authority"** shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.
- 1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

## **2. Processing of Association Personal Data**

### **2.1 The Processor shall:**

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

### **2.2 The Association**

- 2.2.1 Instructs the Processor (and authorises Processor to instruct each Subprocessor) to:
  - 2.2.1.1 *Process Association Personal Data; and*
  - 2.2.1.2 *in particular, transfer Association Personal Data to any country or territory,*as reasonably necessary for the provision of the Services and consistent with the Principal Agreement/Contract; and
- 2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.

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

### **3. Processor and Personnel**

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

### **4. Security**

- 4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in relation to the Association Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.
- 4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

### **5. Subprocessing**

- 5.1 The Association authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.
- 5.2 The Processor may continue to use those Subprocessors already engaged by the Processor as at the date of this Addendum, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.
- 5.3 The Processor shall give the Association prior written notice of its intention to appoint a Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. The Processor shall not appoint (nor disclose any Association Personal Data to) the proposed Subprocessor except with the prior written consent of the Association.
- 5.4 With respect to each Subprocessor, the Processor or the relevant shall:
  - 5.4.1 before the Subprocessor first Processes Association Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level

- of protection for Association Personal Data required by the Principal Agreement;
- 5.4.2 ensure that the arrangement between on the one hand (a) the Processor, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Association Personal Data as those set out in this Addendum and meet the requirements of article 28(3) of the GDPR;
- 5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Processor or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes Association Personal Data; and
- provide to the Association for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as the Association may request from time to time.
- 5.5 The Processor shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Association Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of the Processor.

## **6. Data Subject Rights**

- 6.1 Taking into account the nature of the Processing, the Processor shall assist the Association by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Association's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.
- 6.2 The Processor shall:
- 6.2.1 promptly notify the Association if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Association Personal Data; and
- 6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Association or as required by Applicable Laws to which the Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform

the Association of that legal requirement before the Contracted Processor responds to the request.

## **7. Personal Data Breach**

- 7.1 The Processor shall notify the Association without undue delay upon the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting the Association Personal Data, providing the Association with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.
- 7.2 The Processor shall co-operate with the Association and at its own expense take such reasonable commercial steps as are directed by the Association to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

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

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

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

- 9.1 Subject to sections 9.2 and 9.3, the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing of Association Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.
- 9.2 Subject to section 9.3, the Association may in its absolute discretion by written notice to the Processor within seven (7) days of the Cessation Date require the Processor to (a) return a complete copy of all Association Personal Data to the Association by secure file transfer in such format as is reasonably notified by the Association to the Processor; and (b) delete and procure the deletion of all other copies of Association Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.
- 9.3 Each Contracted Processor may retain Association Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by

Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

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

## **10. Audit rights**

- 10.1 Subject to sections 10.2 and 10.3, the Processor shall make available the Association on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Association or an auditor mandated by the Association in relation to the Processing of the Association Personal Data by the Contracted Processors.
- 10.2 Information and audit rights of the Association only arise under section 10.1 to the extent that the Principal Agreement/Contract does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law (including, where applicable, article 28(3)(h) of the GDPR).
- 10.3 Where carrying out an audit of Personal Data, the Association shall give the Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:
- 10.3.1 to any individual unless they produce reasonable evidence of identity and authority; or
  - 10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Association undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins



## **11. General Terms**

### ***Governing law and jurisdiction***

- 11.1 The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement/Contract with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and
- 11.2 This Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement/Contract.

### ***Order of precedence***

- 11.3 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 Agreement/Contract.
- 11.4 Subject to section 11.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement/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.***

- 11.5 The Association may:
  - 11.5.1 by giving at least twenty eight (28) days' written notice to the Processor, from time to time make any variations to the terms of the Addendum which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and
  - 11.5.2 propose any other variations to this Addendum which the Association reasonably considers to be necessary to address the requirements of any Data Protection Law.

### ***Severance***

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

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

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

On behalf of 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**

## Appendix 7 DATA SHARING AGREEMENT

between

**Paragon Housing Association**, a Scottish Charity (Scottish Charity Number SC036262), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 2521R(s) and having their Registered Office at Invergrange House, Station Rd, Grangemouth, FK3 8DG (the "Association");

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

- (d) The Association 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
- (e) 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.
- (f) 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 Sensitive 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 the Association 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:

- (d) the Data Protection Act 1998;

- (e) (with effect from 25 May 2018) the General Data Protection Regulation (EU) 2016/679;
- (f) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as may be amended by the proposed Regulation on Privacy and Electronic Communications); and
- (g) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, the proposed Regulation on Privacy and Electronic Communications or 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 the Association 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 written 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 the Association 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 the Association 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 Data Protection Act 1998, in respect of processing undertaken on or before 24 May 2018;
  - (b) the General Data Protection Regulation (EU) 2016/679, in respect of processing undertaken on or after 25 May 2018; and
  - (c) in respect of processing undertaken on or after the date on which legislation comes into force that replaces, or enacts into United Kingdom domestic law, the General Data Protection Regulation (EU) 2016/679, that legislation;
- 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 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 is signed; or (iv) if by fax, the date and time of the fax receipt.

## **8 GOVERNING LAW**

- 8.1 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 the Association

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

\_\_\_\_\_  
Director/Secretary/Authorised  
Signatory

before this witness

\_\_\_\_\_  
Print Full Name

\_\_\_\_\_  
Witness

Address

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

\_\_\_\_\_  
**THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN  
THE ASSOCIATION AND #[PARTY 2]**

## **SCHEDULE PART 1 – DATA**

***Drafting Note: This Part should contain details of the Personal Data to be shared between Parties and will need to be populated on a case by case basis when utilising this Agreement.***

### **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 #[insert details].

### **Legal Basis**

#[insert details - this will require specific requirements to be drafted in to the model Agreement depending on the relationship between the Association and Party 2]

### **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
- Secure FTP

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

- Password Protected
- AES Encryption
- SSL / TLS FTP



**SCHEDULE PART 4 – REPRESENTATIVES**

**Contact Details**

**Association**

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:

- Network Username
- Network Password
- Application Username
- Application Password
- Application Permissions and access restricted to those who require it
- Software updates must be applied to servers
- Firewall(s) must be kept up to date

### **3 Disposal of Assets**

3.1 Where information supplied by a Party no longer requires to be retained, any devices containing Personal Data should be physically destroyed or the information should 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.

## **SCHEDULE PART 6 – DATA GOVERNANCE**

### **Data accuracy**

The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

In the event that any information, in excess of information reasonably required in order to allow both organisations to comply with their obligations, is shared, the Data Recipient will notify the other party immediately and arrange the secure return of the information and secure destruction of any copies of that information.

### **Data retention and deletion rules**

The Parties shall independently determine what is appropriate in terms of their own requirements for data retention.

Both Parties acknowledge that Data that is no longer required by either organisation will be securely removed from its systems and any printed copies securely destroyed.